AVG AntiVirus 2015

User Manual

Document revision 2015.35 (26.8.2015)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
All other trademarks are the property of their respective owners.

Contents

1. Introduction **3**

2. AVG Installation Requirements **4**

2.1 Operation Systems Supported 4

2.2 Minimum & Recommended Hardware Requirements 4

3. AVG Installation Process **5**

3.1 Welcome: Language Selection 5

3.2 Welcome: License Agreement 6

3.3 Activate your license 7

3.4 Select type of installation 8

3.5 Custom options 9

3.6 Install progress 10

3.7 Congratulations! 11

4. After Installation **12**

4.1 Virus database update 12

4.2 Product registration 12

4.3 Access to user interface 12

4.4 Scanning of the whole computer 12

4.5 Eicar test 12

4.6 AVG default configuration 13

5. AVG User Interface **14**

5.1 Upper Line Navigation 15

5.2 Security Status Info 18

5.3 Components Overview 19

5.4 My Apps 20

5.5 Scan / Update Quick Links 20

5.6 System Tray Icon 20

5.7 AVG Advisor 22

5.8 AVG Accelerator 23

6. AVG Components **24**

6.1 Computer Protection 24

6.2 Web Browsing Protection 27

6.3 Identity Protection 29

6.4 Email Protection 30

6.5 PC Analyzer 31

7. AVG Advanced Settings **33**

7.1 Appearance 33

7.2 Sounds 35

7.3 Temporarily disable AVG protection 36

7.4 Computer Protection 37
7.5 Email Scanner 41
7.6 Web Browsing Protection 50
7.7 Identity Protection 53
7.8 Scans 54
7.9 Schedules 59
7.10 Update 66
7.11 Exceptions 69
7.12 Virus Vault 72
7.13 AVG Self Protection 73
7.14 Privacy Preferences 73
7.15 Ignore Error Status 75
7.16 Advisor - Known Networks 75

8. AVG Scanning 77
8.1 Predefined Scans 78
8.2 Scanning in Windows Explorer 88
8.3 Command Line Scanning 88
8.4 Scan Scheduling 91
8.5 Scan Results 97
8.6 Scan results details 98

9. AVG File Shredder 100

10. Virus Vault 101

11. History 103
11.1 Scan results 103
11.2 Resident Shield Results 104
11.3 Identity Protection Results 107
11.4 Email Protection Results 108
11.5 Online Shield Results 109
11.6 Event History 111

12. AVG Updates 112
12.1 Update launch 112
12.2 Update levels 112

13. FAQ and Technical Support 114

1. Introduction

This user manual provides comprehensive user documentation for **AVG AntiVirus 2015**.

AVG AntiVirus 2015 offers real-time protection against today's most sophisticated threats. You can chat, download and exchange files with confidence; play games and watch videos without worry or interruption; download, share files and send messages safely; enjoy your life on social networks, or surf and search with of a real-time protection.

You may also want to use other sources of information:

- ***Help file***: A *Troubleshooting* section is available directly in the help file included with **AVG AntiVirus 2015** *(to open the help file, press F1 key in any dialog in the application)*. This section provides a list of the most frequently occurring situations when a user desires to look up professional help for a technical issue. Please select the situation that best describes your problem, and click it to open detailed instructions leading to the problem solution.

- ***AVG website support center***: Alternatively, you can look up the solution to your problem on the AVG website (*http://www.avg.com/*). In the ***Support*** section you can find an overview of thematic groups dealing with both sales and technical issues, a structured section of frequently asked questions, and all available contacts.

- ***AVG ThreatLabs***: A specific AVG related website (*http://www.avg.com/about-viruses*) is dedicated to virus issues providing structured overview of information related to online threats. You can also find instructions on removing viruses, spyware, and advice on how to stay protected.

- ***Discussion forum***: You can also use the AVG users discussion forum at http://community.avg.com/.

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG AntiVirus 2015 is intended to protect workstations with the following operating systems:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (all editions)
- Windows 7 (all editions)
- Windows 8 (all editions)
- Windows 10 (all editions)

(and possibly higher service packs for specific operating systems)

***Note**: The Identity component is not supported on Windows XP x64. On this operating system you can install AVG AntiVirus 2015 but only without the IDP component.*

2.2. Minimum & Recommended Hardware Requirements

Minimum hardware requirements for **AVG AntiVirus 2015**:

- Intel Pentium CPU 1.5 GHz or faster
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) of RAM memory
- 1.3 GB of free hard drive space *(for installation purposes)*

Recommended hardware requirements for **AVG AntiVirus 2015**:

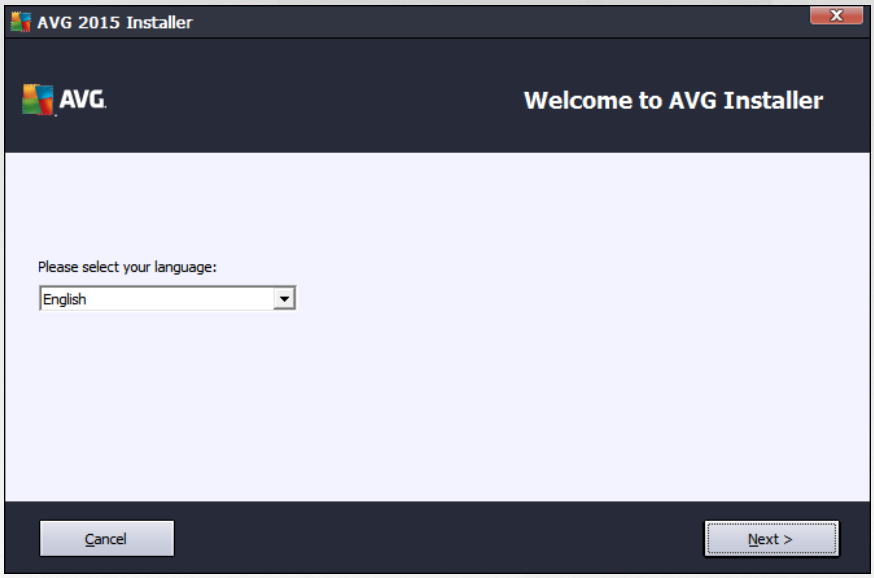
- Intel Pentium CPU 1.8 GHz or faster
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) of RAM memory
- 1.6 GB of free hard drive space *(for installation purposes)*

3. AVG Installation Process

To install **AVG AntiVirus 2015** on your computer, you need to get the latest installation file. To make sure you are installing the up-to-date version of **AVG AntiVirus 2015**, it is recommended that you download the installation file from the AVG website (http://www.avg.com/). The ***Support*** section provides a structured overview of the installation files for each AVG edition. Once you have downloaded and saved the installation file on your hard disk, you can launch the installation process. The installation is a sequence of simple and easy to understand dialogs. Each dialog briefly describes what do at each step of the installation process. We offer a detailed explanation of each dialog window below:

3.1. Welcome: Language Selection

The installation process starts with the ***Welcome to AVG Installer*** dialog:

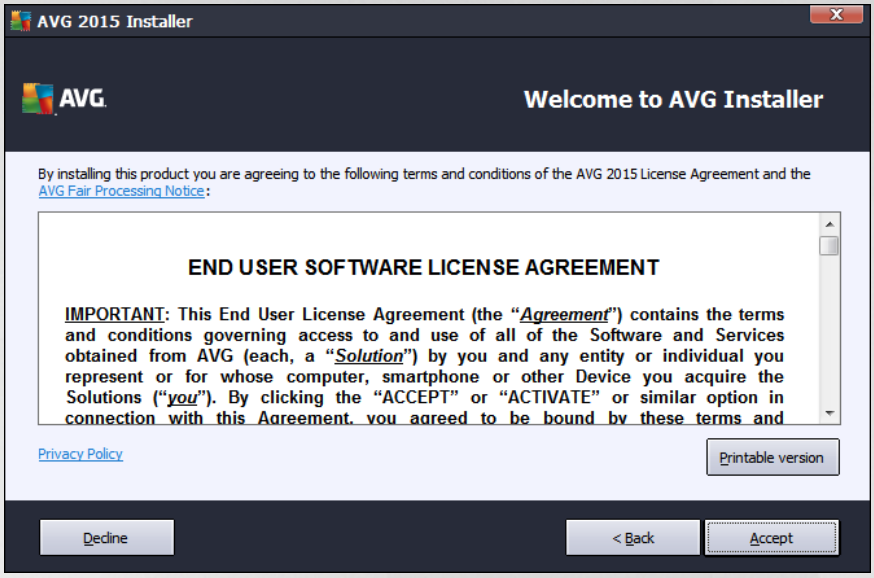


In this dialog you can select the language used for the installation process. Click the combo box to roll down the language menu. Select the desired language, and the installation process will proceed further in the language of your choice.

Attention: At the moment you are only selecting the language of the installation process. The AVG AntiVirus 2015 application will be installed in the selected language, and in English which is always installed automatically. However, it is possible to have more languages installed and to work with AVG AntiVirus 2015 in any of these. You will be invited to confirm your full selection of alternative languages in one of following setup dialogs named Custom Options.

3.2. Welcome: License Agreement

The ***Welcome to AVG Installer*** dialog provides then the full wording of the AVG license agreement:



Please read the entire text carefully. To confirm that you have read, understood, and accept the agreement press the ***Accept*** button. If you do not agree with the license agreement press the ***Decline*** button, and the installation process will be terminated immediately.

AVG Fair Processing Notice and Privacy Policy

Besides the license agreement, this setup dialog also offers you the option to learn more about ***AVG Fair Processing Notice***, and ***Privacy Policy***. The mentioned functions are displayed in the dialog in the form of an active hyperlink that takes you to the dedicated website where you can find detailed information. Click the respective link to get redirected to AVG website (http://www.avg.com/) where you can find the full wording of these statements.

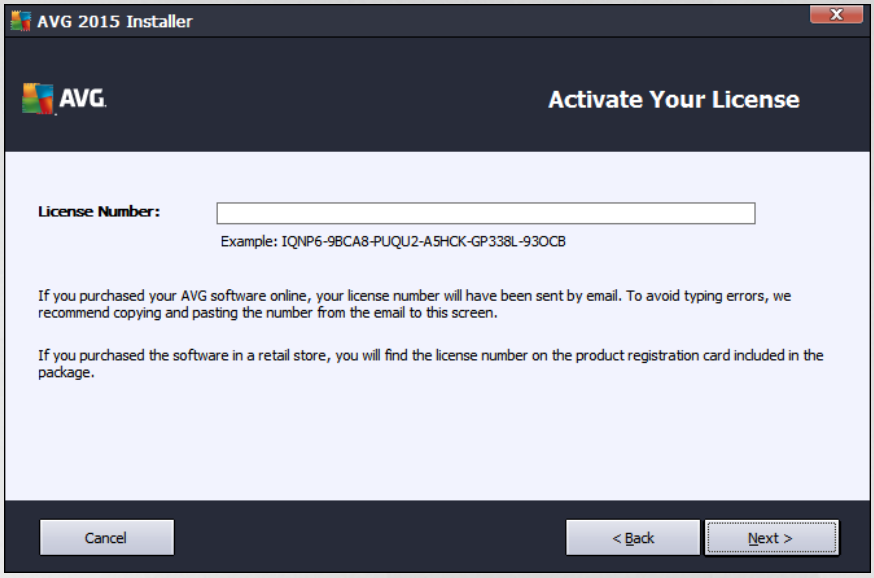
Control buttons

From the first setup dialog, the following control buttons are available:

- ***Printable version*** - Click the button to display the full wording of the AVG license agreement in a web interface, and well arranged for printing.
- ***Decline*** - Click to refuse the license agreement. The setup process will quit immediately. **AVG AntiVirus 2015** will not be installed!
- ***Back*** - Click to return one step back to the previous setup dialog.
- ***Accept*** - Click to confirm you have read, understood, and accepted the license agreement. The installation will continue, and you will go on one step further to the following setup dialog.

3.3. Activate your license

In the ***Activate Your License*** dialog you are invited to enter your license number into the provided text field:



Where to find the license number

The sales number can be found on the CD packaging in your **AVG AntiVirus 2015** box. The license number will be in the confirmation email that you received after purchasing your **AVG AntiVirus 2015** online. You must type in the number exactly as shown. If the digital form of the license number is available (*in the email*), it is recommended that you use the copy and paste method to insert it.

How to use the Copy & Paste method

Using the ***Copy & Paste*** method to enter your **AVG AntiVirus 2015** license number into the program ensures that the number is correctly entered. Please follow these steps:

- Open the email containing your license number.
- Click the left mouse button at the beginning of the license number, hold and drag the mouse to the end of the number, and then release the button. The number should now be highlighted.
- Press and hold ***Ctrl***,and then press ***C***. This copies the number.
- Point and click the position where you would like to paste the copied number.
- Press and hold ***Ctrl***,and then press ***V***. This pastes the number to the location you selected.

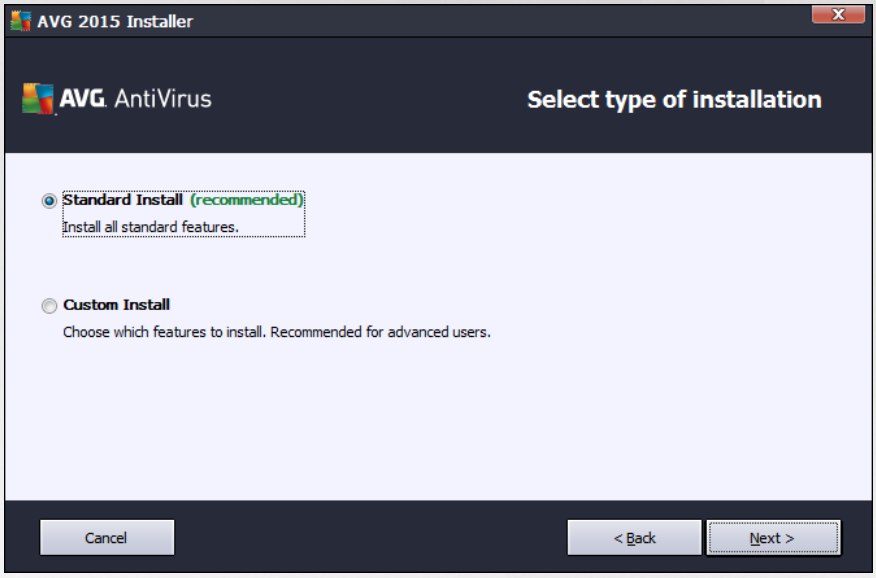
Control buttons

As in most setup dialogs, there are three control buttons available:

- ***Cancel*** - click to exit the setup process immediately; **AVG AntiVirus 2015** will not be installed!
- ***Back*** - click to go one step back to the previous setup dialog.
- ***Next*** - click to continue the installation and go one step further.

3.4. Select type of installation

The ***Select type of installation*** dialog offers the choice of two installation options: ***Standard*** and ***Custom Install***:



Standard installation

For most users, it is highly recommended that you keep the standard ***Standard*** installation. This way you install **AVG AntiVirus 2015** in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the option of doing so directly in the **AVG AntiVirus 2015** application.

Press the ***Next*** button to proceed to the following dialog of the installation process.

Custom installation

Custom Install should only be used by experienced users who have a valid reason to install **AVG AntiVirus 2015** with non-standard settings; e.g. to fit specific system requirements. If you decide for this way, a new option of ***Destination folder*** will be activated in the dialog. Here, you are supposed to specify the location where **AVG AntiVirus 2015** should be installed. By default, **AVG AntiVirus 2015** will be installed to the program files folder located on drive C:, as stated in the text field in the dialog. If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective folder. To revert to the default destination previously set by the software vendor use the ***Default*** button.

Then, press the ***Next*** button to proceed to the Custom Options dialog.

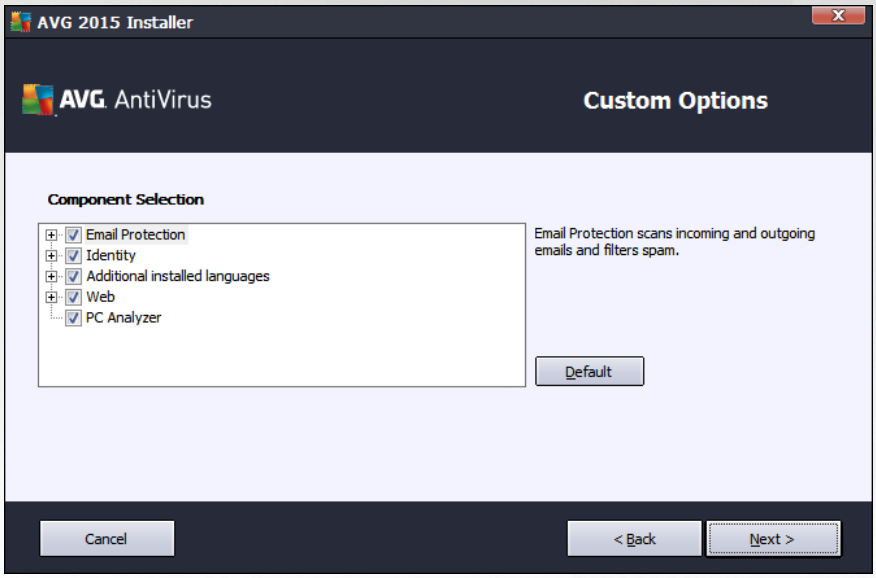
Control buttons

As within most setup dialogs, there are three control buttons available:

- ***Cancel*** - click to exit the setup process immediately; **AVG AntiVirus 2015** will not be installed!
- ***Back*** - click to go one step back to the previous setup dialog.
- ***Next*** - click to continue the installation and go one step further.

3.5. Custom options

The ***Custom Options*** dialog allows you to set up detailed parameters for the installation:



The ***Component Selection*** section provides an overview of all **AVG AntiVirus 2015** components that can be installed. If the default settings do not suit you, you can remove/add specific components. ***However, you can only select from components that are included in your purchased AVG edition!*** Highlight any item in the ***Component Selection*** list, and a brief description of the respective component will be displayed on the right side of this section. For detailed information on each component's functionality please consult the Components Overview chapter of this documentation. To revert to the default configuration pre-set by the software vendor use the ***Default*** button.

In this step, you can also decide to install other then default language variants of the product *(by default, the application gets installed in the language you have selected as you setup communication language, and in English)*.

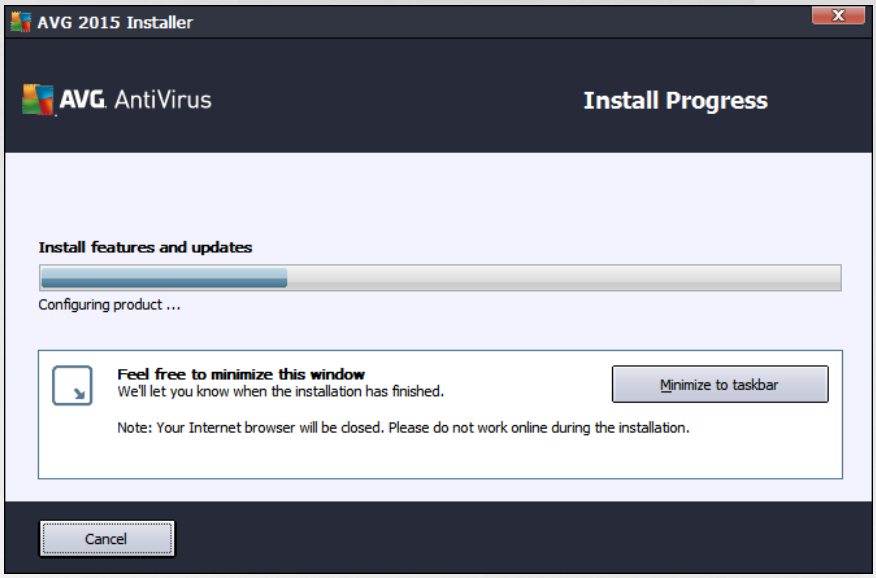
Control buttons

As in most setup dialogs, there are three control buttons available:

- ***Cancel*** - click to exit the setup process immediately; **AVG AntiVirus 2015** will not be installed!
- ***Back*** - click to go one step back to the previous setup dialog.
- ***Next*** - click to continue the installation and go one step further.

3.6. Install progress

The ***Install Progress*** dialog shows the progress of the installation process, and does not require any intervention:



After the installation process is finished, you will be automatically redirected to the next dialog.

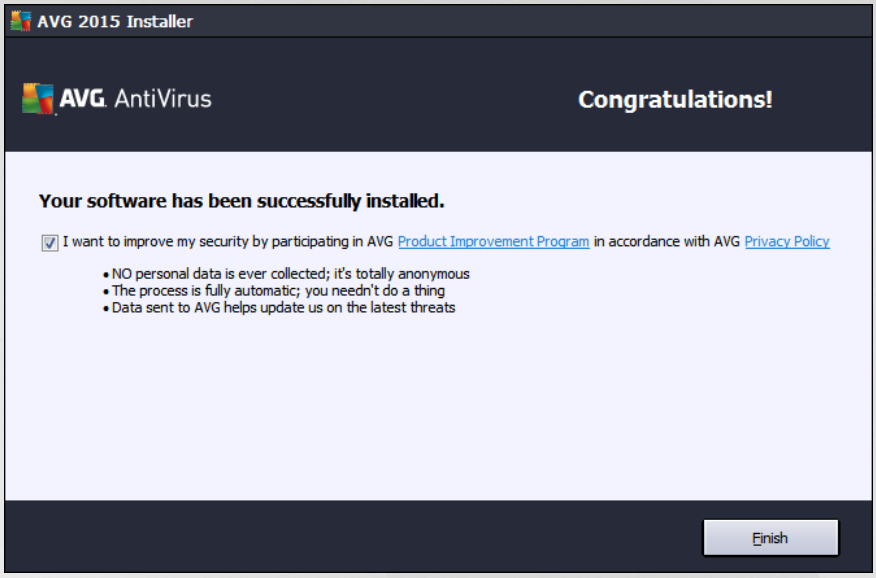
Control buttons

There are two control buttons available in this dialog:

- ***Minimize*** - The installation process may take several minutes. Click the button to minimize the dialog window into an icon visible on the system bar. The dialog appears again once the installation is completed.
- ***Cancel*** - This button should only be used if you want to stop the current installation process. Please mind that in such a case your **AVG AntiVirus 2015** will not be installed!

3.7. Congratulations!

The ***Congratulations*** dialog confirms that your **AVG AntiVirus 2015** has been fully installed and configured:



Product Improvement Program and Privacy Policy

Here you can decide whether you want to participate in the ***Product Improvement Program*** (*for details see the chapter AVG Advanced Settings / Product Improvement Program*) that collects anonymous information on detected threats in order to increase the overall Internet security level. All data are treated as confidential and in compliance with AVG Privacy Policy; click the ***Privacy Policy*** link to get redirected to AVG website (http://www.avg.com/) where you can find the the full wording of AVG Privacy Policy. If you agree, please keep the option checked *(the option is confirmed, by default)*.

To finalize the installation process press the ***Finish*** button.

4. After Installation

4.1. Virus database update

Please note that upon installation *(after computer restart, if required)*, **AVG AntiVirus 2015** automatically updates its virus database and all components, putting them to full working order, which can take a couple of minutes. While the update process is running, you will be notified about the fact by the information displayed in the main dialog. Please wait for a while to finish the update process, and have your **AVG AntiVirus 2015** completely up and ready to protect you!

4.2. Product registration

Having finished the **AVG AntiVirus 2015** installation, please register you product online on the AVG website (*http://www.avg.com/*). After the registration you will be able to gain full access to your AVG user account, the AVG Update newsletter, and other services provided exclusively for registered users. The easiest way to register is directly from the **AVG AntiVirus 2015** user interface. Please select the upper line navigation / Options / Register now item. You will be redirected to the ***Registration*** page on the AVG website (*http://www.avg.com/*). Please follow the instruction provided on the page.

4.3. Access to user interface

The AVG main dialog is accessible in several ways:

- double-click the AVG system tray icon
- double-click the AVG icon on the desktop
- from the menu ***Start / All Programs / AVG / AVG 2015***

4.4. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG AntiVirus 2015** installation. For this reason you should run a Scan of the whole computer to make sure there are no infections on your PC. The first scan might take quite some time *(about an hour)* but it is recommended that you launch it to make sure your computer has not been compromised by a threat. For instructions on running a Scan of the whole computer consult the chapter AVG Scanning.

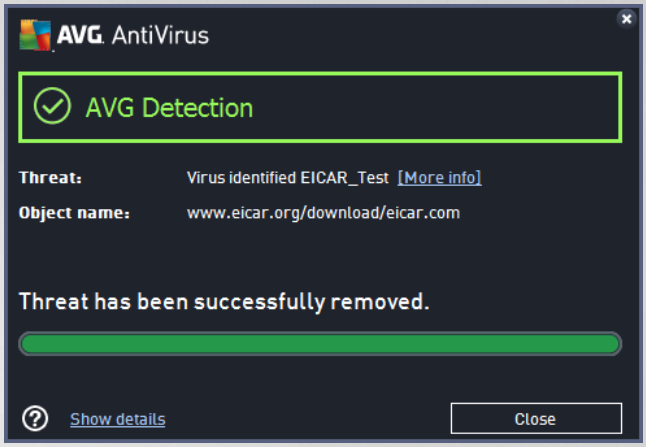
4.5. Eicar test

To confirm that **AVG AntiVirus 2015** has been installed correctly you can perform the EICAR test.

The EICAR test is a standard and absolutely safe method used to test antivirus system operation. It is safe to pass around, because it is not an actual virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (*though they typically report it with an obvious name, such as "EICAR-AV-Test"*). You can download the EICAR virus from the EICAR website at www.eicar.com, and you will also find all necessary EICAR test information there.

Try to download the *eicar.com* file, and save it on your local disk. Immediately after you confirm downloading of the test file, your **AVG AntiVirus 2015** will react to it with a warning. This notice demonstrates that AVG is

correctly installed on your computer.



If AVG fails to identify the EICAR test file as a virus, you should check the program configuration again!

4.6. AVG default configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG AntiVirus 2015** is set by the software vendor so that all components and functions are tuned up to achieve optimum performance. ***Unless you have a real reason to do so, do not change the AVG configuration! Changes to settings should only be performed by an experienced user.*** If you want to change the AVG configuration to better suit your needs, go to AVG Advanced Settings: select the main menu item *Options/Advanced settings*, and edit the AVG configuration in the newly opened AVG Advanced Settings dialog.

5. AVG User Interface

AVG AntiVirus 2015 opens with the main window:



The main window is divided into several sections:

- ***Upper line navigation*** consists of four active links lined up in the upper section of the main window *(Like AVG, Reports, Support, Options).* Details >>
- ***Security Status Info*** provides basic information on the current status of your **AVG AntiVirus 2015**. Details >>
- ***Installed components overview*** can be found in a horizontal strip of blocks in the central section of the main window. The components are displayed as light green blocks labeled by the respective component icon, and provided with the information on the component status. Details >>
- ***My Apps*** are graphically depicted in the lower central strip of the main window and offer you an overview of applications complementary to **AVG AntiVirus 2015** that are either already installed on your computer, or recommended for installation. Details >>
- ***Scan / Fix / Update quick links*** are placed in the lower line of blocks in the main window. These buttons allow an immediate access to the most important and most frequently used AVG functions. Details >>

Outside the main window of **AVG AntiVirus 2015**, there is one more control element that you might use to access the application:

- ***System tray icon*** is located in the bottom right-hand corner of the monitor *(on the system tray),* and indicates the current status of **AVG AntiVirus 2015**. Details >>

5.1. Upper Line Navigation

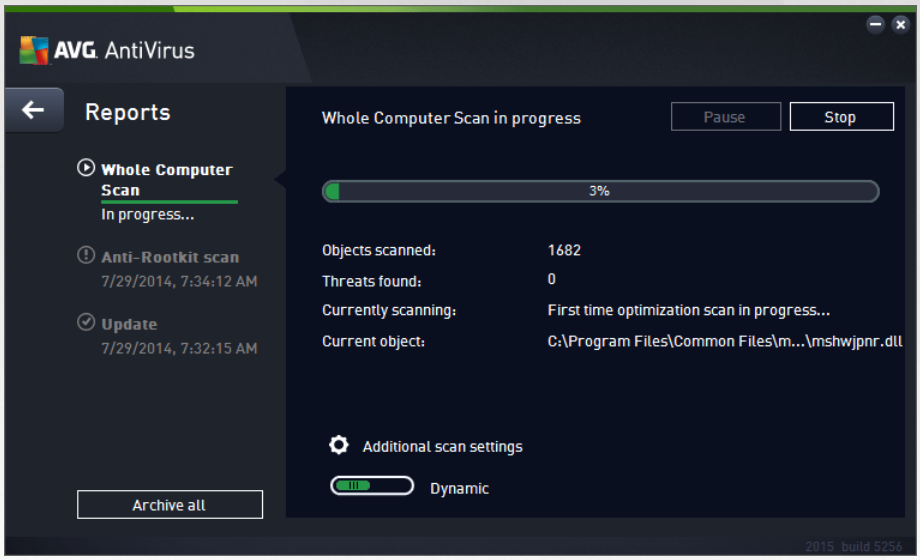
The ***Upper line navigation*** consists of several active links lined up in the upper section of the main window. The navigation includes the following buttons:

5.1.1. Join us on Facebook

Single click the link to get connected to the AVG Facebook community and to share the latest AVG information, news, tips and tricks for your maximum internet security.

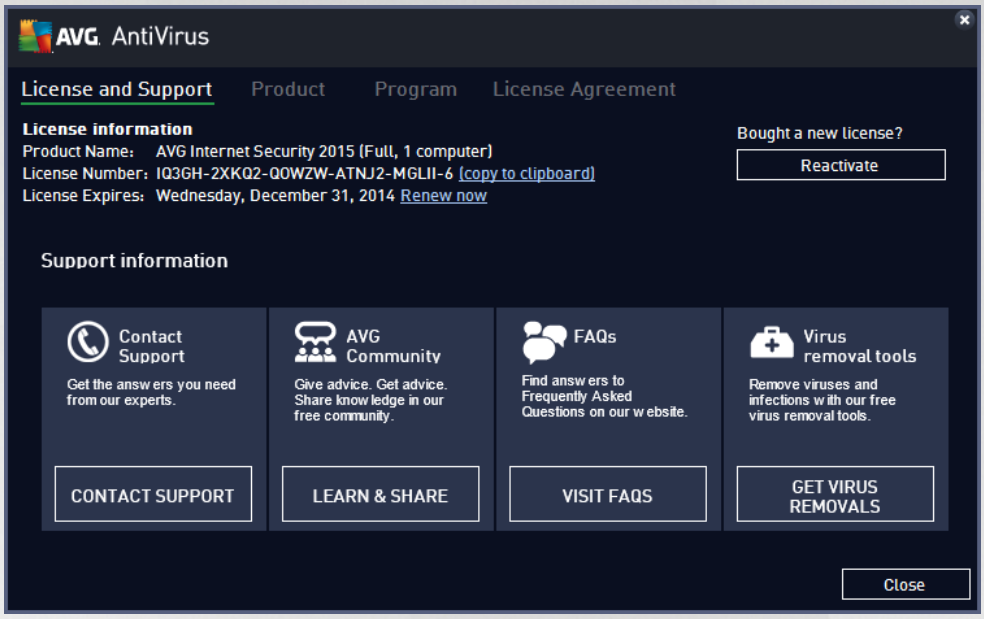
5.1.2. Reports

Opens a new ***Reports*** dialog with an overview of all relevant reports on previously launched scans and update processes. If the scan or update is currently running, a rotating circle will be displayed next to the ***Reports*** text in the upper navigation of the main user interface. Click this circle to get to the dialog depicting the progress of the running process:



5.1.3. Support

Opens a new dialog structured into four tabs where you can find all relevant information about **AVG AntiVirus 2015**:



- ***License and Support*** - The tab provides information on the product name, the license number, and the expiration date. In the bottom section of the dialog you can also find a clearly arranged overview of all available contacts to customer support. The following active links and buttons are available in the tab:

    - *(Re)Activate* - Click to open the new ***AVG Activate Software*** dialog. Fill in your license number into the respective field to either replace your sales number *(that you use during the AVG AntiVirus 2015 installation)*, or to change your current license number for another *(e.g. when upgrading to a higher AVG product)*.

    - *Copy to clipboard* - Use this link to copy the license number, and paste it where needed. This way you can be sure the license number is entered correctly.

    - *Renew now* - We recommend that you purchase your **AVG AntiVirus 2015** license renewal in good time, at least one month prior to your current license expiration. You will be noticed of the approaching expiration date. Click this link to get redirected to AVG website *(http://www.avg.com/)* where you find detailed information on your license status, the expiration date, and the renewal/upgrade offer.

- ***Product*** - The tab provides an overview of the **AVG AntiVirus 2015** most important technical data referring to product information, installed components, and installed email protection.

- ***Program*** - On this tab you can find information on the program file version, and on the third parties code used in the product.

- ***License Agreement*** - The tab offers the full wording of the license agreement between you and AVG Technologies.

5.1.4. Options

The maintenance of **AVG AntiVirus 2015** is accessible via the ***Options*** item. Click the arrow to open the roll-down menu:

- ***Scan computer*** launches a scan of the whole computer.
- ***Scan selected folder...*** - Switches to the AVG scanning interface and allows you to define within the tree structure of your computer which files and folders should be scanned.
- ***Scan file...*** - Allows you to run an on-demand test on a single specific file. Click this option to open a new window with the tree structure of your disk. Select the desired file, and confirm the scan launch.
- ***Update*** - Automatically launches the update process for **AVG AntiVirus 2015**.
- ***Update from directory...*** - Runs the update process from the update files located in a specified folder on your local disk. However, this option is only recommended as an emergency, e.g. in situations where there is no connection to the Internet (for example, your computer is infected and disconnected from the Internet; your computer is connected to a network with no access to the Internet, etc.). In the newly opened window select the folder where you have previously placed the update file, and launch the update process.
- ***Virus Vault*** - Opens the interface to the quarantine space, Virus Vault, to where AVG removes all detected infections. Inside this quarantine the infected files are isolated, your computer's security is guaranteed, and at the same time the infected files are stored for possible future repair.
- ***History*** - Offers further specific submenu options:
  - *Scan results* - Opens a dialog providing an overview of scanning results.
  - *Resident Shield Results* - Opens a dialog with an overview of threats detected by Resident Shield.
  - *Identity Protection Results* - Opens a dialog with an overview of threats detected by Identity component.
  - *Email Protection Results* - Opens a dialog with an overview of mail messages attachments detected as dangerous by the Email Protection component.
  - *Online Shield Results* - Opens a dialog with an overview of threats detected by Online Shield.
  - *Event history log* - Opens the history log interface with an overview of all logged **AVG AntiVirus 2015** actions.
- ***Advanced settings...*** - Opens the AVG advanced settings dialog where you can edit the **AVG AntiVirus 2015** configuration. Generally, it is recommended that you keep the default settings of the application as defined by the software vendor.
- ***Help contents*** - Opens the AVG help files.
- ***Get support*** - Opens the support dialog providing all accessible contacts and support information.
- ***Your AVG Web*** - Opens the AVG website (*http://www.avg.com/*).

- ***About Viruses and Threats*** - Opens the online virus encyclopedia on AVG website (*http://www.avg.com/*) where you can look up detailed information on the identified virus.

- ***(Re)Activate*** - Opens the activation dialog with the license number you have provided during the installation process. Within this dialog you can edit your license number to either replace the sales number (*you have installed AVG with*), or to replace the old license number (*e.g. when upgrading to a new AVG product*). If using the trial version of **AVG AntiVirus 2015**, the latter two items appear as ***Buy now*** and ***Activate***, allowing you to buy the full version of the program right away. For **AVG AntiVirus 2015** installed with a sales number, the items display as ***Register*** and ***Activate***:

- ***Register now / MyAccount*** - Connects to the registration page of the AVG website (*http://www.avg.com/*). Please fill in your registration data; only customers who register their AVG product can receive free technical support.

- ***About AVG*** - Opens a new dialog with four tabs providing data on your purchased license and accessible support, product and program information, and the full wording of the license agreement. *(The same dialog can be opened via the Support link of the main navigation.)*

5.2. Security Status Info

The ***Security Status Info*** section is located in the upper part of the **AVG AntiVirus 2015** main window. Within this section you will always find information on the current security status of your **AVG AntiVirus 2015**. Please see an overview of icons possibly depicted in this section, and their meaning:

 - the green icon indicates that your ***AVG AntiVirus 2015 is fully functional***. Your computer is completely protected, up-to-date, and all installed components are working properly.

 - the yellow icon warns that ***one or more components are incorrectly configured*** and you should check their properties/settings. There is no critical problem in **AVG AntiVirus 2015** and you have probably decided to switch a component off for some reason. You are still protected!. However, please pay attention to the problem component's settings! The incorrectly configured component will be displayed with a warning orange strip in the main user interface.

The yellow icon also appears if for some reason you have decided to ignore a component's error status. The ***Ignore error status*** option is accessible in the Advanced settings / Ignore error status branch. There you have the option to state you are aware of the component's error state but for some reason you wish to keep your **AVG AntiVirus 2015** so and you do not want to be warned about it. You may need to use this option in a specific situation but it is strictly recommended that you switch the ***Ignore error status*** option off as soon as possible!

Alternatively, the yellow icon will also be displayed if your **AVG AntiVirus 2015** requires a computer restart (***Restart needed***). Please pay attention to this warning and restart your PC.

 - the orange icon indicates that ***AVG AntiVirus 2015 is in a critical status***! One or more components do not work properly and **AVG AntiVirus 2015** cannot protect your computer. Please pay immediate attention to fixing the reported problem! If you are not able to fix the error yourself, contact the AVG technical support team.

In case AVG AntiVirus 2015 is not set to the optimum performance, a new button named Click to fix (alternatively Click to fix it all if the problem involves more than one component) appears next to the security status information. Press the button to launch an automatic process of checking and

configuring the program. This is an easy way to set AVG AntiVirus 2015 to the optimum performance and reach the maximum security level!

It is strongly recommended that you pay attention to ***Security Status Info*** and if the report indicates any problem, go ahead and try to solve it immediately. Otherwise your computer is at risk!

Note: *AVG AntiVirus 2015 status information can also be obtained at any time from the system tray icon.*

5.3. Components Overview

Installed components overview can be found in a horizontal strip of blocks in the central section of the main window. The components are displayed as light green blocks labeled by the respective component icon. Each block provides information on the current status of protection. If the component is configured correctly and fully functional, the information is stated in green letters. If the component is stopped, its functionality is limited, or the component is in error state, you will be notified by a warning text displayed in an orange text field. ***It is strictly recommended that you pay attention to the respective component's settings!***

Move the mouse over the component to display a short text at the bottom of the main window. The text provides an elementary introduction to the component's functionality. Also, it informs on the component's current status, and specifies which of the component's services is not configured correctly.

Installed components' list

Within the **AVG AntiVirus 2015** the ***Components Overview*** section contains information on the following components:

- ***Computer*** - This components covers two services: ***AntiVirus Shield*** detects viruses, spyware, worms, trojans, unwanted executable files, or libraries within your system, and protects you from malicious adware, and ***Anti-Rootkit*** scans for dangerous rootkits hidden inside applications, drivers, or libraries. Details >>
- ***Web Browsing*** - Protects you from web-based attacks while you search and surf the Internet. Details >>
- ***Identity*** - The component runs the ***Identity Shield*** service that is constantly protecting your digital assets from new and unknown threats on the Internet. Details >>
- ***Emails*** - Checks your incoming email messages for SPAM, and blocks viruses, phishing attacks, or other threats. Details >>

Actions accessible

- ***Move mouse over any component's icon*** to highlight it within the components overview. At the same time, the component's basic functionality description appears in the bottom part of the user interface.
- ***Single-click component's icon*** to open the component's own interface with the information on the component's current status, and access to its configuration and statistical data.

5.4. My Apps

In the ***My Apps*** area *(the line of green blocks under the components set)* you can find an overview of additional AVG applications that are either already installed on your computer, or recommended for installation. The blocks are displayed conditionally, and may represent any of the following applications:

- ***Mobile protection*** is an application that protects your cell phone from viruses and malware. It also provides you with the ability of tracking your smart phone remotely if you should become separated from it.
- ***LiveKive*** is dedicated to online data backup on secured servers. LiveKive automatically backs up all your files, photos, and music to one safe place, allowing you to share them with family and friends and access them from any web-enabled device, including iPhones and Android devices.
- ***Family Safety*** helps you protect your children from inappropriate websites, media content, and online searches, and provides you with reports regarding their online activity. AVG Family Safety uses key-stroke technology to monitor your child's activities in chat-rooms and on social networking sites. If it spots words, phrases or language that are known to be used to victimize children online, it will notify you immediately via SMS or email. The application allows you to set the appropriate level of protection for each of your children, and monitor them separately via unique logins.
- ***PC Tuneup*** application is an advanced tool for detailed system analysis and correction, as to how the speed and overall performance of your computer might be improved.

For detailed information on any of the ***My Apps*** applications click the respective block. You will get redirected to the dedicated AVG webpage, where you can also download the component immediately.

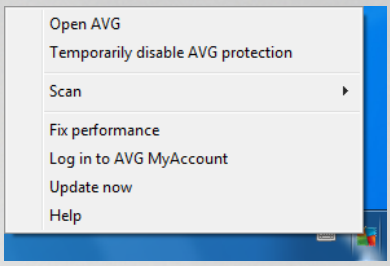
5.5. Scan / Update Quick Links

Quick links are located in the lower line of buttons in the **AVG AntiVirus 2015** user interface. These links allow you to immediately access the most important and most frequently used features of the application, i.e. scanning and update. The quick links are accessible from all dialogs of the user interface:

- ***Scan now*** - The button is graphically divided into two sections. Follow the ***Scan now*** link to launch the Whole Computer Scan immediately, and watch its progress and results in the automatically opened Reports window. The ***Options*** button opens the ***Scan Options*** dialog where you can manage scheduled scans and edit parameters of the Whole Computer Scan / Scan of Specific Files or Folders. *(For details see chapter AVG Scanning)*
- ***Fix performance*** - The button takes you to the ***PC Analyzer*** service, an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved.
- ***Update now*** - Press the button to launch the product update immediately. You will be informed about the update results in the slide dialog over the AVG system tray icon. *(For details see chapter AVG Updates)*

5.6. System Tray Icon

The ***AVG System Tray Icon*** *(on your Windows taskbar, right-hand bottom corner of your monitor)* indicates the current status of your **AVG AntiVirus 2015**. It is visible at all times in your system tray, no matter whether the user interface of your **AVG AntiVirus 2015** is opened or closed:



AVG System Tray Icon display

- In full color with no added elements the icon indicates that all **AVG AntiVirus 2015** components are active and fully functional. However, the icon can also be displayed this way in a situation when one of the components is not fully functional but the user has decided to ignore the component state. *(Having confirmed the ignore for component state option you express, you are aware of the component's error state but for some reason you wish to keep it so, and you do not want to be warned about the situation.)*

- The icon with an exclamation mark indicates that a component *(or even more components)* is in error state. Always pay attention to such a warning and try to remove the configuration issue for a component that is not set up properly. In order to be able to perform the changes in the component's configuration, double-click the system tray icon to open the application user interface. For detailed information on which components is in error state please consult the security status info section.

- The system tray icon can further be displayed in full color with a flashing and rotating beam of light. This graphic version signalizes a currently launched update process.

- The alternative display of a full color icon with an arrow means that one of the **AVG AntiVirus 2015** scans is running now.

AVG System Tray Icon information

The ***AVG System Tray Icon*** also informs about current activities within your **AVG AntiVirus 2015**, and on possible status changes in the program (*e.g. automatic launch of a scheduled scan or update, a component's status change, error status occurrence, ...*) via a pop-up window opened from the system tray icon.

Actions accessible from AVG System Tray Icon

AVG System Tray Icon can also be used as a quick link to access the user interface of **AVG AntiVirus 2015**; just double-click the icon. By right-click the icon you open a brief context menu with the following options:

- ***Open AVG*** - click to open the user interface of **AVG AntiVirus 2015**.

- ***Temporarily disable AVG protection*** - the option allows you to switch off the entire protection secured by your **AVG AntiVirus 2015** at once. Please remember that you should not use this option unless it is absolutely necessary! In most cases, it is not necessary to disable **AVG AntiVirus 2015** before installing new software or drivers, not even if the installer or software wizard suggests that running programs and applications be shut down first to make sure there are no unwanted

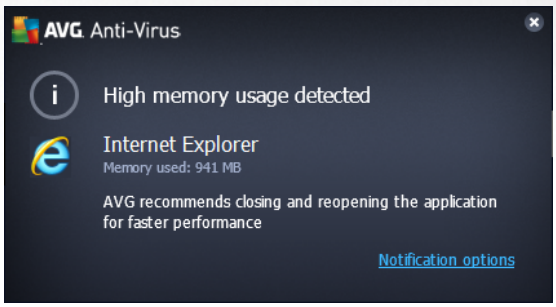
interruptions during the installation process. If you do have to temporarily disable **AVG AntiVirus 2015**, you should re-enable it as soon as you're done. If you are connected to the Internet or a network during the time your antivirus software is disabled, your computer is vulnerable to attacks.

- ***Scan*** - click to open the context menu for predefined scans (*Whole Computer scan, and Scan Specific Files or Folders*) and select the required scan; it will be launched immediately.
- ***Running scans ...*** - this item is displayed only if a scan is currently running on your computer. For this scan you can then set its priority, alternatively stop or pause the running scan. The following actions are also accessible: *Set priority for all scans, Pause all scans* or *Stop all scans*.
- ***Fix performance*** - click to launch the PC Analyzer component.
- ***Log in to AVG MyAccount*** - Opens the MyAccount homepage where you can manage your subscription products, purchase additional protection, download installation files, check your past orders and invoices, and manage your personal information.
- ***Update now*** - launches an immediate update.
- ***Help*** - opens the help file on the start page.

5.7. AVG Advisor

AVG Advisor has been designed to detect problems that might be slowing your computer down, or putting it at risk, and to recommend an action to solve the situation. If you see a sudden computer slowdown *(Internet browsing, overall performance)*, it is not usually obvious what exactly the culprit is, and subsequently, how to solve the problem. That is where ***AVG Advisor*** comes in: It will display a notification in the system tray informing you what the problem might be, and suggesting how to fix it. ***AVG Advisor*** keeps monitoring all running processes within your PC for possible issues, and offering tips on how to avoid the problem.

AVG Advisor is visible in the form of a sliding pop-up over the system tray:



Specifically, ***AVG Advisor*** monitors the following:

- ***The state of any currently opened web browser***. Web browsers may overload the memory, especially if multiple tabs or windows have been opened for some time, and consume too much of system resources, i.e. slowing down your computer. In such situation, restarting the web browser usually helps.
- ***Running Peer-To-Peer connections***. After using the P2P protocol for sharing files, the connection can sometimes remain active, using up certain amount of your bandwidth. As a result, you can see web browsing slowdown.

- ***Unknown network with a familiar name***. This usually only applies to users who connect to various networks, typically with portable computers: If a new, unknown network has the same name as a well-known, frequently used network *(e.g. Home or MyWifi)*, confusion can occur, and you can accidentally connect to a completely unknown and potentially unsafe network. ***AVG Advisor*** can prevent this by warning you that the known name actually represents a new network. Of course, if you decide that the unknown network is safe, you can save it to an ***AVG Advisor*** list of known networks so that it is not reported again in the future.

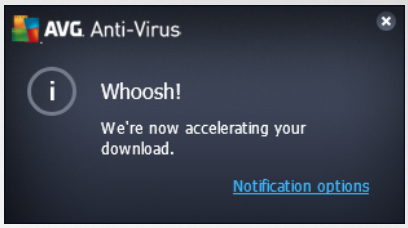
In each of these situation, ***AVG Advisor*** warns you of the possible problem that might occur, and it provides the name and icon of the conflicting process, or application. Also, ***AVG Advisor*** suggests what steps should be taken to avoid the possible problem.

Supported web browsers

The feature works with the following web browsers: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

AVG Accelerator allows smoother online video playback and makes additional downloads easier. When the video-acceleration process is in progress, you will be notified via the system tray pop-up window.



6. AVG Components

6.1. Computer Protection

The ***Computer*** component covers two main security services: ***AntiVirus*** and ***Data Safe***:

- ***AntiVirus*** consists of a scanning engine that guards all files, the system areas of the computer, and removable media *(flash disk etc.)* and scans for known viruses. Any detected virus will be blocked from taking any action, and will then be cleaned or quarantined in the Virus Vault. You do not even notice the process, as this so called resident protection runs "in the background". AntiVirus also uses heuristic scanning, where files are scanned for typical virus characteristics. This means that the AntiVirus can detect a new, unknown virus, if the new virus contains some typical characteristics of existing viruses. **AVG AntiVirus 2015** is also able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system *(various kinds of spyware, adware etc.)*. Furthermore, AntiVirus scans your system registry for suspicious entries, temporary Internet files, and allows you to treat all potentially unwanted items in the same way as any other infection.

- ***Data Safe*** enables you to create secure virtual vaults to store valuable or sensitive data in. The contents of a Data Safe are encrypted and protected with a password of your choice so that nobody can access it without authorization.



Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(AntiVirus or Data Safe)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which

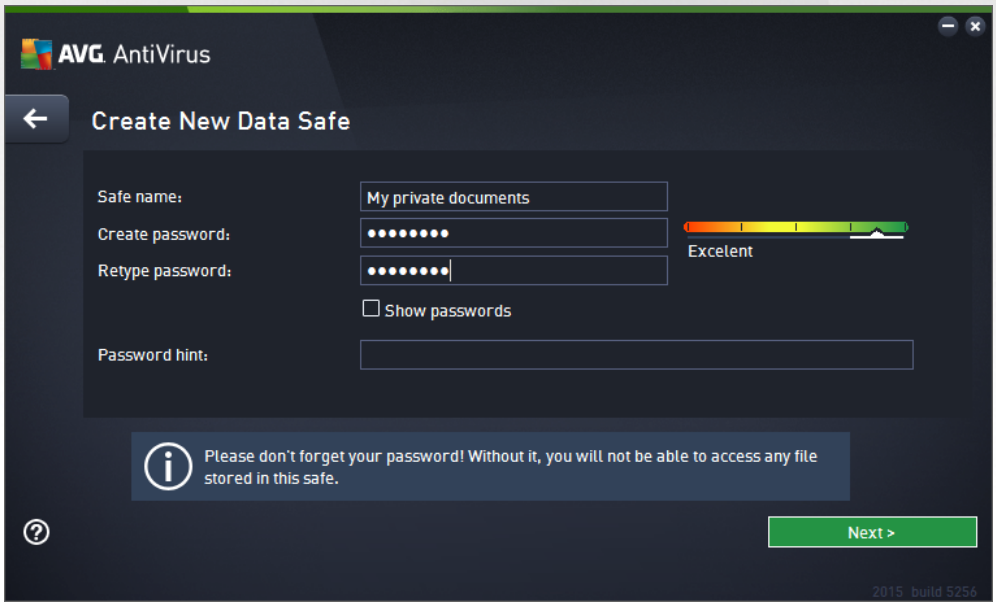
means that the AntiVirus security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. AntiVirus. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

How to create your data safe

In the ***Data Safe*** section of the ***Computer Protection*** dialog you can find the ***Create Your Safe*** button. Click the button to open a new dialog of the same name where you can specify the parameters of your planned safe. Please fill in all necessary information, and follow the instructions in the application:



First, you have to specify your safe's name, and create a strong password:

- ***Safe name*** - To create a new data safe, you first need to choose a suitable safe name to recognize it. If you share the computer with other family members, you might want to include your name as well as indication of the safe contents, for example *Dad's emails*.

- ***Create password / Retype password*** - Create password for your data safe and type it in the respective text fields. The graphic indicator on the right will tell you if your password is weak *(relatively easy to break with special software tools)* or strong. We recommend choosing a password of at least medium strength. You can make your password stronger by including uppercase letters, numbers and

other characters such as dots, dashes, etc. If you want to make sure that you type the password as intended, you can check the ***Show password*** box *(of course, nobody else should be looking at your screen)*.

- ***Password hint*** - We strongly recommend that you also create a helpful password hint that will remind you what your password is in case you forget. Remember that a Data Safe is designed to keep your files secure by only allowing access with the password; there are no workarounds for this, and if you forget the password, you will not be able to access your data safe!

Having specified all required data in the text fields, click the ***Next*** button to continue to the next step:



This dialog provides the following configuration options:

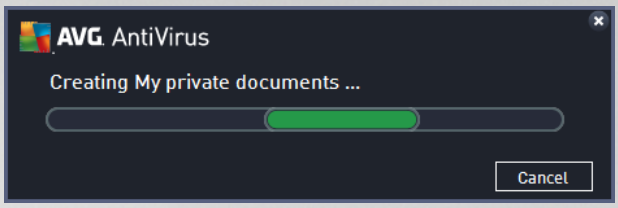
- ***Location*** states where the data safe will be physically placed. Browse for a suitable destination on your hard drive, or you can keep the predefined location, which is your *Documents* folder. Please note that once you create a data safe, you cannot change its location.

- ***Size*** - you can predefine the size of your data safe, which will allocate the necessary space on the disk. The value should be set to be neither too small *(not enough for your needs)*, nor too big *(taking up too much disk space uselessly)*. If you already know what you want to put in the data safe, you can place all the files in one folder and then use the ***Select a folder*** link to automatically calculate the total size. However, the size can be changed later on according to your needs.

- ***Access*** - the checkboxes in this section enable you to create convenient shortcuts to your data safe.

How to use your data safe

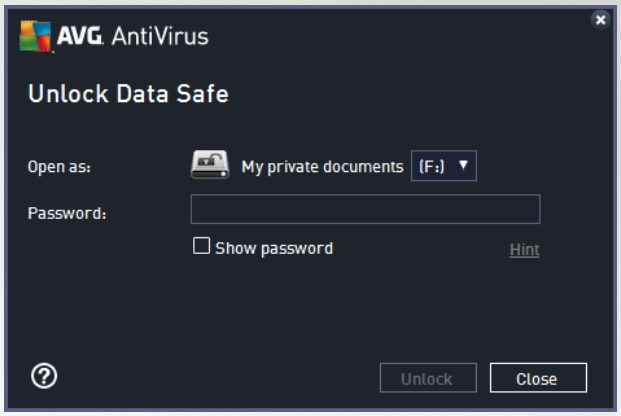
Once you are happy with the settings, click the ***Create Safe*** button. A new dialog ***Your Data Safe is now ready*** pops up announcing the safe is available for storing your files in. Right now the safe is open and you can access it immediately. With every next attempt to access the safe you will be invited to unlock the safe with the password you have defined:



To use your new data safe, you need to open it first - click the ***Open Now*** button. Upon opening, the data safe appears in your computer as a new virtual disk. Please assign it a letter of your choice from the drop-down menu (*you will only be allowed to select from currently free disks*). Typically, you will not be allowed to choose C *(assigned usually to your hard drive)*, A *(floppy disk drive)*, or D *(DVD drive)*. Please note that each time you unlock a data safe, you can choose a different available drive letter.

How to unlock your data safe

With your next attempt to access the data safe you will be invited to unlock the safe with the password you have defined:



In the text field, please type your password to authorize yourself, and click the ***Unlock*** button. If you need help remembering the password, click ***Hint*** to display the password hint that you defined when creating the data safe. The new data safe will appear in the overview of your data safes as UNLOCKED, and you will be able to add/remove files in it as required.

6.2. Web Browsing Protection

The ***Web Browsing Protection*** consists of two services: ***LinkScanner Surf-Shield*** and ***Online Shield***:

- ***LinkScanner Surf-Shield*** protects you from the increasing number of 'here today, gone tomorrow' threats on the web. These threats can be hidden on any type of website, from governments to big, well-known brands to small businesses, and they rarely stick around on those sites for more than 24 hours. LinkScanner protects you by analyzing the web pages behind all the links on any web page you're viewing and making sure they're safe at the only time that matters - when you're about to click that link. ***LinkScanner Surf-Shield is not intended for server platforms protection!***

- ***Online Shield*** is a type of a real time resident protection; it scans the content of visited web pages (and possible files included in them) even before these are displayed in your web browser or downloaded to your computer. Online Shield detects that the page you are about to visit includes

some dangerous javascript, and prevents the page from being displayed. Also, it recognizes malware contained in a page and stops its downloading immediately so that it never gets to your computer. This powerful protection will block malicious content of any web page you try to open, and prevent it from being downloaded to your computer. With this feature enabled, clicking a link or typing in a URL to a dangerous site will automatically block you from opening the web page thus protecting you from inadvertently being infected. It is important to remember that exploited web pages can infect your computer simply by visiting the affected site. ***Online Shield is not intended for server platforms protection!***



Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(LinkScanner Surf-Shield or Online Shield)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the LinkScanner Surf-Shield / Online Shield security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

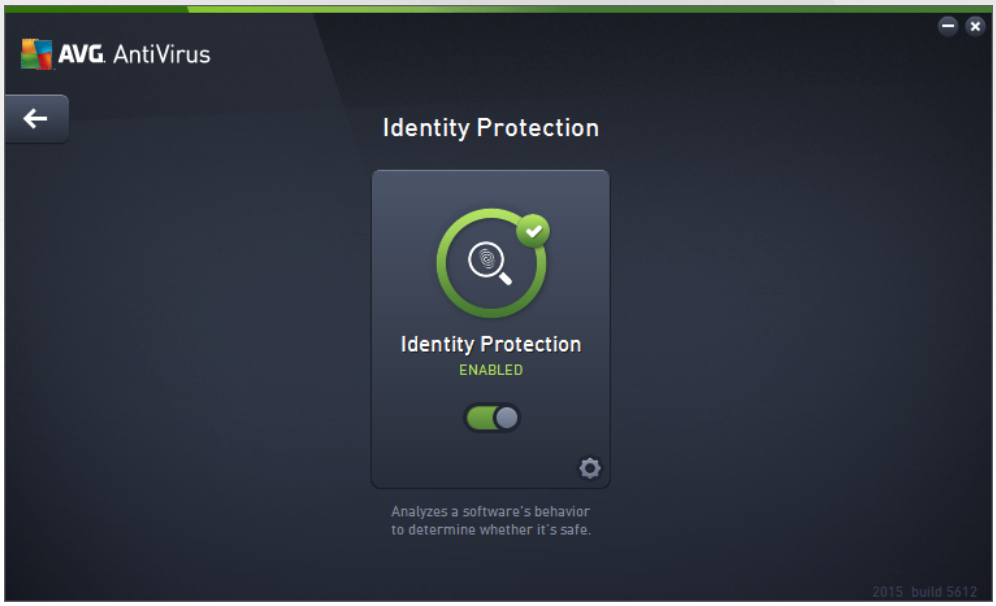
Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. LinkScanner Surf-Shield or Online Shield. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

6.3. Identity Protection

The ***Identity Protection*** component runs the ***Identity Shield*** service that is constantly protecting your digital assets from new and unknown threats on the Internet:

- ***Identity Protection*** is an anti-malware service that protects you from all kinds of malware (*spyware, bots, identity theft, ...*) using behavioral technologies and provide zero day protection for new viruses. Identity Protection is focused on preventing identity thieves from stealing your passwords, bank account details, credit card numbers and other personal digital valuables from all kinds of malicious software *(malware)* that target your PC. It makes sure that all programs running on your PC or in your shared network are operating correctly. Identity Protection spots and blocks suspicious behavior on a continuous basis and protects your computer from all new malware. Identity Protection gives your computer a realtime protection against new and even unknown threats. It monitors all *(including hidden)* processes and over 285 different behaviour patterns, and can determine if something malicious is happening within your system. For this reason, it can reveal threats not even yet described in the virus database. Whenever an unknown piece of code comes onto your computer, it is immediately watched for malicious behaviour, and tracked. If the file is found to be malicious, Identity Protection will remove the code into the Virus Vault and undo any changes that have been made to the system *(code injections, registry changes, ports opening etc)*. You do not need to initiate a scan to be protected. The technology is very proactive, rarely needs updating, and is always on guard.



Dialog controls

In the dialog, you can find the following controls:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the Identity Protection security service is active and fully functional. The red color represents

the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

 ***Settings*** - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. Identity Protection. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus 2015** but any configuration can be recommended to experienced users only!

 ***Arrow*** - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

Unfortunately, in **AVG AntiVirus 2015** the Identity Alert service is not included. If you like to use this type of protection, follow the ***Upgrade to Activate*** button to get redirected to the dedicated webpage where you can purchase the Identity Alert license.

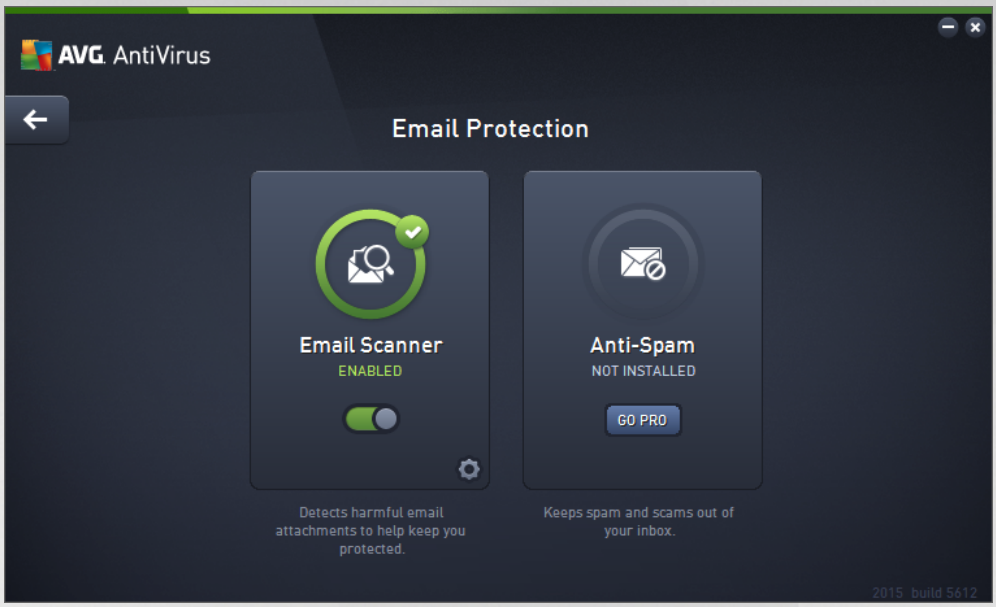
Please mind that even with the AVG Premium Security editions, the Identity Alert service is currently available in selected regions only: US, United Kingdom, Canada, and Ireland.

6.4. Email Protection

The ***Email Protection*** component covers the following two security services: ***Email Scanner*** and ***Anti-Spam*** *(the Anti-Spam service is only accessible in the Internet / Premium Security editions)*.

- ***Email Scanner***: One of the most common sources of viruses and trojans is via email. Phishing and spam make email an even greater source of risks. Free email accounts are more likely to receive such malicious emails *(as they rarely employ anti-spam technology)*, and home users rely quite heavily on such email. Also home users, surfing unknown sites and filling in online forms with personal data *(such as their email address)*, increase exposure to attacks via email. Companies usually use corporate email accounts and employ anti-spam filters etc, to reduce the risk. The Email Protection component is responsible for scanning every email message sent or received; whenever a virus is detected in an email, it is removed to the Virus Vault immediately. The component can also filter out certain types of email attachments, and add a certification text to infection-free messages. ***Email Scanner is not intended for server platforms!***

- ***Anti-Spam*** checks all incoming email messages and marks unwanted emails as spam *(Spam refers to unsolicited email, mostly advertising a product or service that is mass mailed to a huge number of email addresses at the same time, filling recipients' mail boxes. Spam does not refer to legitimate commercial email for which consumers have given their consent.)*. Anti-Spam can modify the subject of the email *(that has been identified as spam)* by adding a special text string. You can then easily filter your emails in your email client. The Anti-Spam component uses several analysis methods to process each email message, offering maximum possible protection from unwanted email messages. Anti-Spam uses a regularly updated database for the detection of spam. It is also possible to use RBL servers *(public databases of "known spammer" email addresses)* and to manually add email addresses to your Whitelist *(never mark as spam)* and Blacklist *(always mark as spam)*.



Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(Email Scanner or Anti-Spam)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. Email Scanner or Anti-Spam. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

6.5. PC Analyzer

The ***PC Analyzer*** component is an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved. It opens via the ***Fix performance*** button located in the main user interface dialog or via the same option listed in the context menu of the system tray AVG icon. You will then be able to watch the analysis progress and its results directly in the chart:



The following categories can be analyzed: registry errors, junk files, fragmentation, and broken shortcuts:

- ***Registry Errors*** will give you the number of errors in Windows Registry that might be slowing your computer down, or causing error messages to appear.
- ***Junk Files*** will give you the number of files that use up your disk space, and can most likely be deleted. Typically, these will be many kinds of temporary files, and files in the Recycle Bin.
- ***Fragmentation*** will calculate the percentage of your hard disk that is fragmented, i.e. used for a long time so that most files are now scattered over different parts of the physical disk.
- ***Broken Shortcuts*** will find shortcuts that no longer work, lead to non-existing locations etc.

The results overview provides the number of detected system problems classified according to the respective categories tested. The analysis results will also be displayed graphically on an axis in the ***Severity*** column.

Control buttons

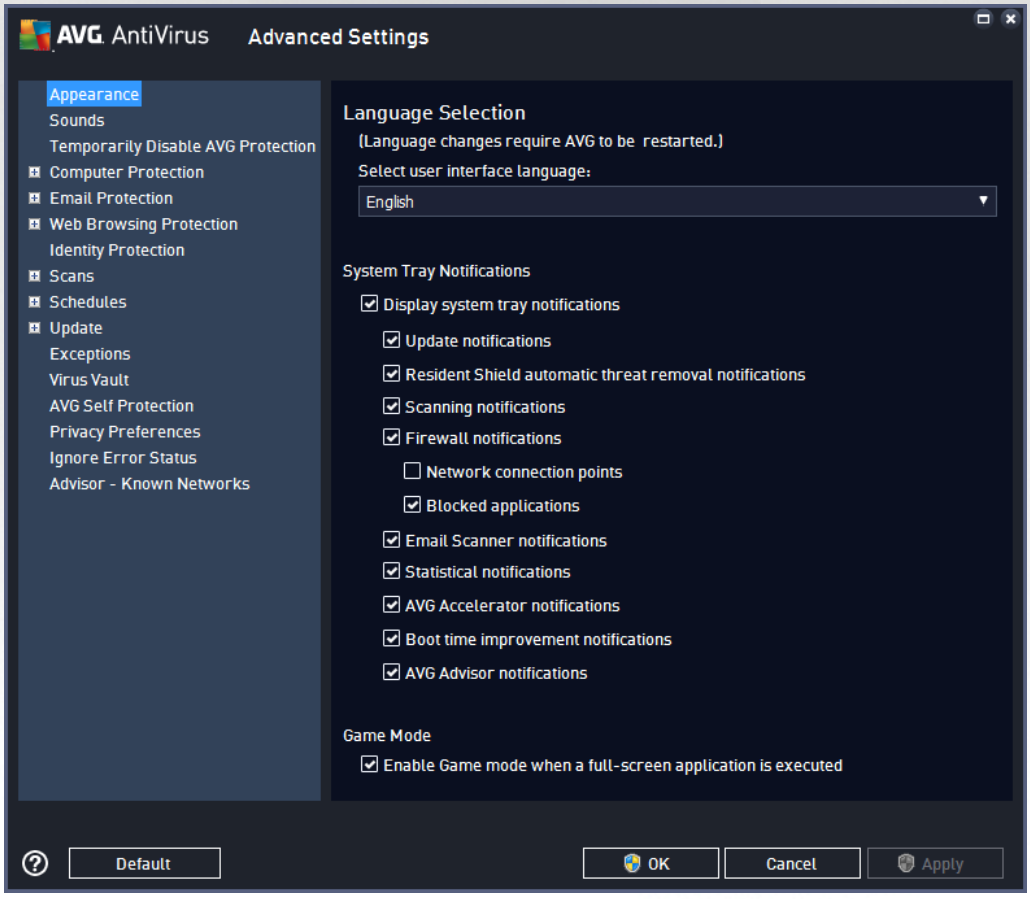
- ***Stop analysis*** (*displayed while the analysis is running*) - press this button to interrupt the analysis of your computer.
- ***Fix now*** *(displayed once the analysis is finished*) - Unfortunately, the functionality of the PC Analyzer within the **AVG AntiVirus 2015** is limited to your PC present status analysis. However, AVG provides an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved. Click the button to get redirected to the dedicated website for more information.

7. AVG Advanced Settings

The advanced configuration dialog of **AVG AntiVirus 2015** opens in a new window named ***Advanced AVG Settings***. The window is divided into two sections: the left part offers a tree-arranged navigation to the program configuration options. Select the component for which you want to change the configuration (*or its specific part*) to open the editing dialog in the right-hand section of the window.

7.1. Appearance

The first item of the navigation tree, ***Appearance***, refers to the general settings of the **AVG AntiVirus 2015** user interface, and provides a few elementary options of the application's behavior:

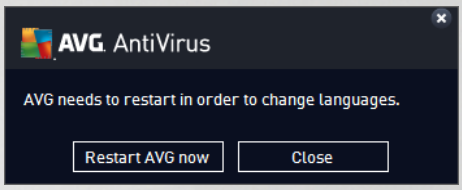


Language selection

In the ***Language selection*** section you can chose your desired language from the drop-down menu. The selected language will then be used for the entire **AVG AntiVirus 2015** user interface. The drop-down menu only offers those languages you have previously selected to be installed during the installation process plus English (*English is always installed automatically, by default*). To finish switching your **AVG AntiVirus 2015** to another language you have to restart the application. Please follow these steps:

- In the drop-down menu, select the desired language of the application
- Confirm your selection by pressing the ***Apply*** button *(right-hand bottom corner of the dialog)*

- Press the ***OK*** button confirm
- A new dialog pops-up informing you that in order to change the language of the application, you need to restart your **AVG AntiVirus 2015**
- Press the ***Restart AVG now*** button to agree with the program restart, and wait a second for the language change to take effect:



System tray notifications

Within this section you can suppress displaying system tray notifications on the status of the **AVG AntiVirus 2015** application. By default, the system notifications are allowed to be displayed. It is highly recommended that you keep this configuration! System notifications provide information for example on launching the scanning or updating process, or on status changes of a **AVG AntiVirus 2015** component. You should certainly pay attention to these notifications!

However, if for some reason you decide that you do not wish to be informed in this way, or that you would like only certain notifications *(related to a specific AVG AntiVirus 2015 component)* to be displayed, you can define and specify your preferences by checking/unchecking the following options:

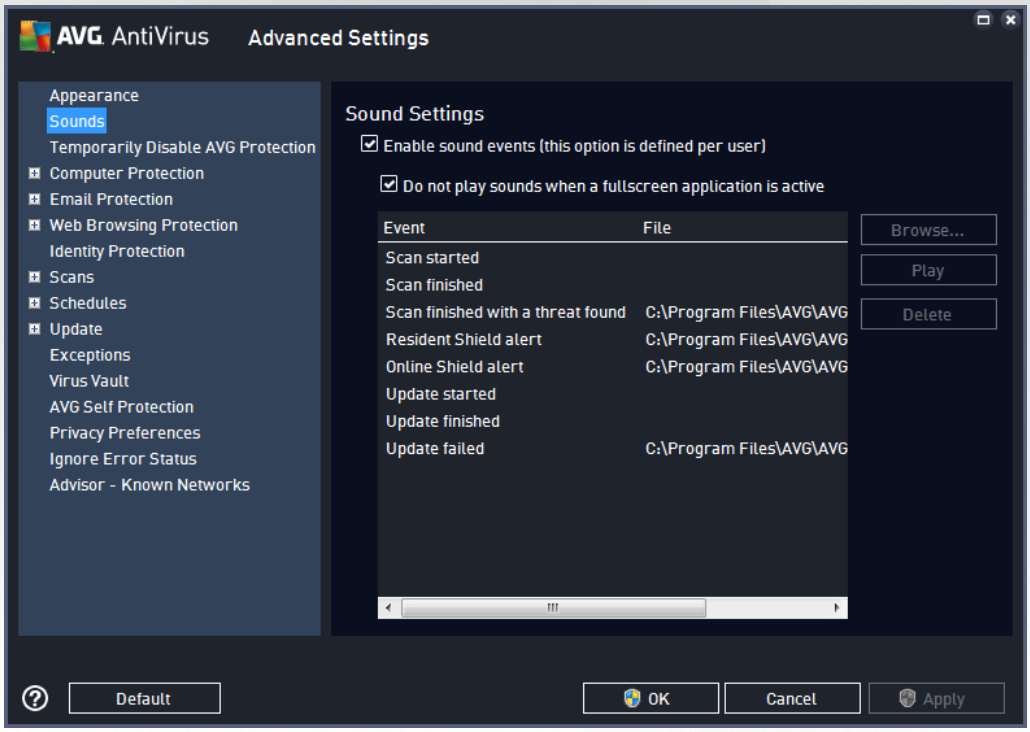
- ***Display system tray notifications*** *(on, by default)* - by default, all notifications are displayed. Uncheck this item to completely turn off the display of all system notifications. When turned on, you can further select what specific notifications should be displayed:
    - ***Update notifications*** *(on, by default)* - decide whether information regarding the **AVG AntiVirus 2015** update process launch, progress, and finalization should be displayed.
    - ***Resident Shield automatic threat removal notifications*** *(on, by default)* - decide whether information regarding file saving, copying, and opening processes should be displayed or suppressed (*this configuration only appears if the Resident Shield auto-heal option is on*).
    - ***Scanning notifications*** *(on, by default)* - decide whether information upon automatic launch of the scheduled scan, its progress, and results should be displayed.
    - ***Email Scanner notifications*** *(on, by default)* - decide whether information on scanning of all incoming and outgoing email messages should be displayed.
    - ***Statistical notifications*** *(on, by default)* - keep the option checked to allow regular statistical review notification to be displayed in the system tray.
    - ***Boot time improvement notifications*** *(off, by default)* - decide whether you wish to be informed about your computer boot time acceleration.
    - ***AVG Advisor notifications*** *(on, by default)* - decide whether information upon AVG Advisor activities should be displayed in the slide panel on the system tray.

Gaming mode

This AVG function is designed for full-screen applications where any AVG information balloons (*displayed e.g. when a scheduled scan is started*) would be disturbing (*they could minimize the application or corrupt its graphics*). To avoid this situation, keep the checkbox for the ***Enable gaming mode when a full-screen application is executed*** option marked (*default setting*).

7.2. Sounds

Within the ***Sound Settings*** dialog you can specify whether you want to be informed about specific **AVG AntiVirus 2015** actions by a sound notification:



The settings are only valid for the current user account. That means, each user on the computer can have their own sound settings. If you want to allow the sound notification, keep the ***Enable sound events*** option checked (*the option is on, by default*) to activate the list of all relevant actions. You may also want to check the ***Do not play sounds when full screen application is active*** option to suppress the sound notification in situations when it might be disturbing *(see also the Gaming mode section of the Advanced settings/Appearance chapter in this document)*.

Control buttons

- ***Browse...*** - having selected the respective event from the list, use the ***Browse*** button to search your disk for the desired sound file you want to assign to it. *(Please note that only *.wav sounds are supported at the moment!)*

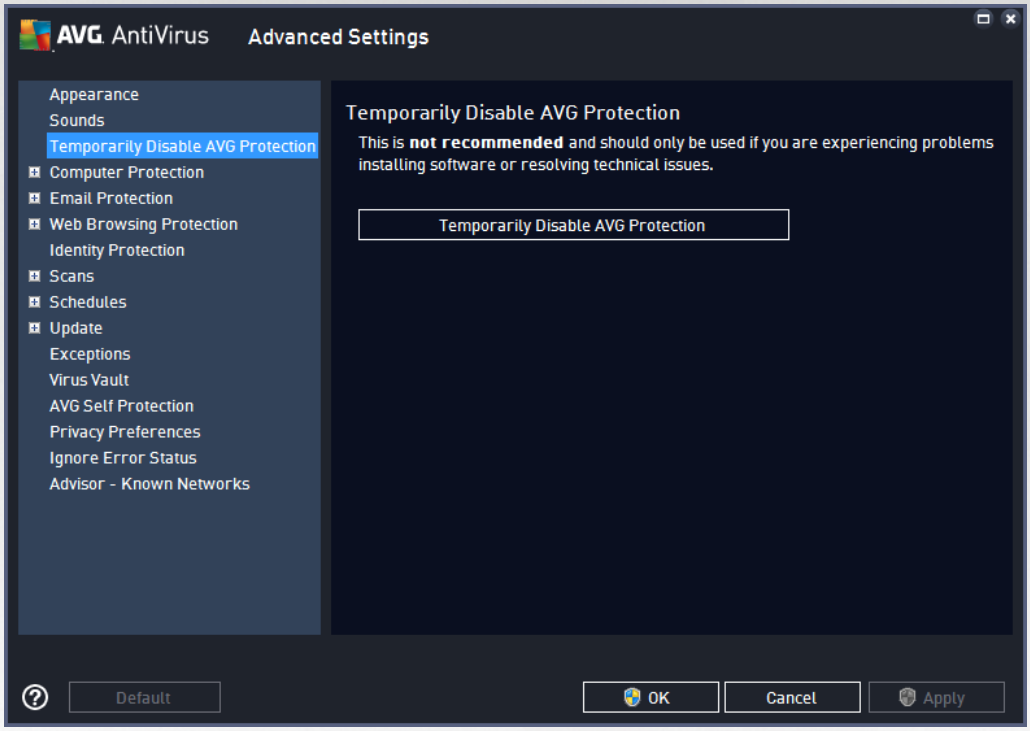
- ***Play*** - to listen to the selected sound, highlight the event in the list and push the ***Play*** button.

- ***Delete*** - use the ***Delete*** button to remove the sound assigned to a specific event.

7.3. Temporarily disable AVG protection

In the ***Temporarily disable AVG protection*** dialog you have the option of switching off the entire protection secured by your **AVG AntiVirus 2015** at once.

Please remember that you should not use this option unless it is absolutely necessary!



In most cases, it is ***not necessary*** to disable **AVG AntiVirus 2015** before installing new software or drivers, not even if the installer or software wizard suggests that running programs and applications be shut down first to make sure there are no unwanted interruptions during the installation process. Should you really experience problems during installation, try to deactivate the resident protection *(in the linked dialog, uncheck the **Enable Resident Shield** item)* first. If you do have to temporarily disable **AVG AntiVirus 2015**, you should re-enable it as soon as you're done. If you are connected to the Internet or a network when your antivirus software is disabled, your computer is vulnerable to attacks.

How to disable AVG protection

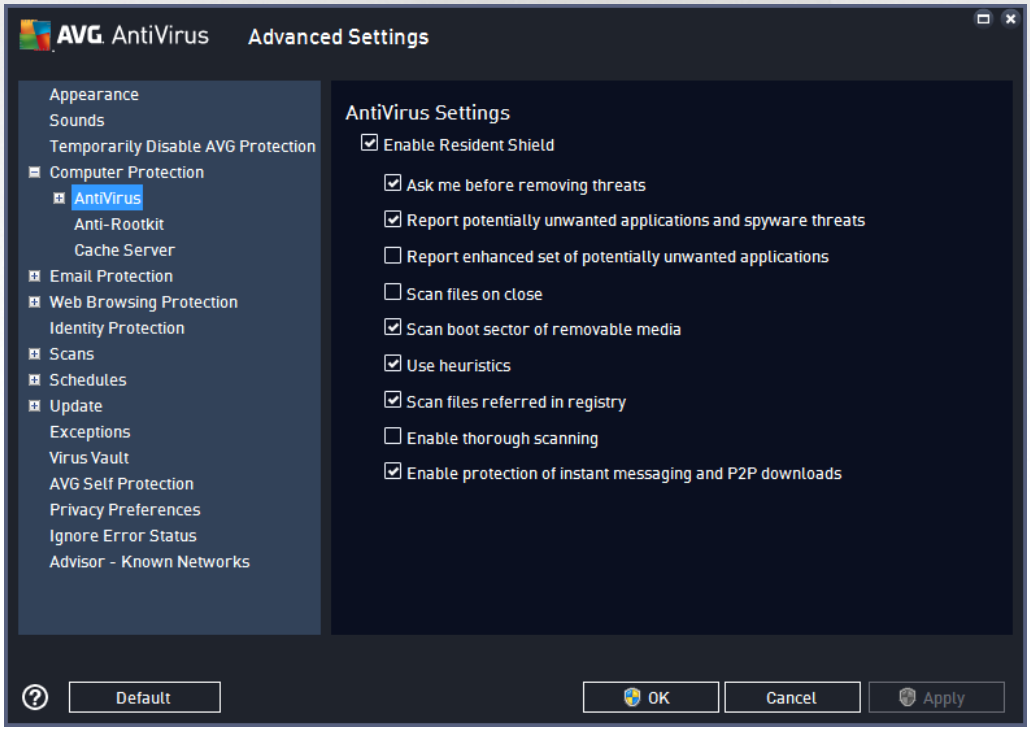
Tick the ***Temporarily disable AVG protection*** checkbox, and confirm your choice by pressing the ***Apply*** button. In the newly open ***Temporarily disable AVG protection*** dialog specify for how long you wish to disable your **AVG AntiVirus 2015**. By default, the protection will be turned off for 10 minutes which should be sufficient for any common task such as installing new software etc. You can decide for a longer time period, however this option is not recommended if not absolutely necessary. Afterwards, all deactivated components will be automatically activated again. At most, you can disable the AVG protection till the next computer restart.



7.4. Computer Protection

7.4.1. AntiVirus

AntiVirus together with ***Resident Shield*** protect your computer continuously from all known types of viruses, spyware, and malware in general *(including so-called sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated)*.



In the ***Resident Shield Settings*** dialog you can activate or deactivate the resident protection completely by checking or unchecking the ***Enable Resident Shield*** item (*this option is switched on by default*). In addition, you can select which features of the resident protection should be activated:

- ***Ask me before removing threats*** (*on by default*) - check to ensure that the Resident Shield will not

perform any action automatically; instead it will display a dialog describing the detected threat, allowing you to decide what should be done. If you leave the box unchecked, **AVG AntiVirus 2015** will automatically heal the infection, and if this is not possible, the object will be moved into the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** (*on by default*) - check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer's security.

- ***Report enhanced set of potentially unwanted applications*** (*off by default*) - mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer's security even more, however it can possibly block legal programs, and is therefore switched off by default.

- ***Scan files on close*** (*off by default*) - on-close scanning ensures that AVG scans active objects (e.g. applications, documents ...) when they are being opened, and also when they are being closed; this feature helps to protect your computer against some types of sophisticated virus.

- ***Scan boot sector of removable media*** (*on by default*) - check to scan boot sectors of any inserted USB flash disks, external disk drives and other removable media for threats.

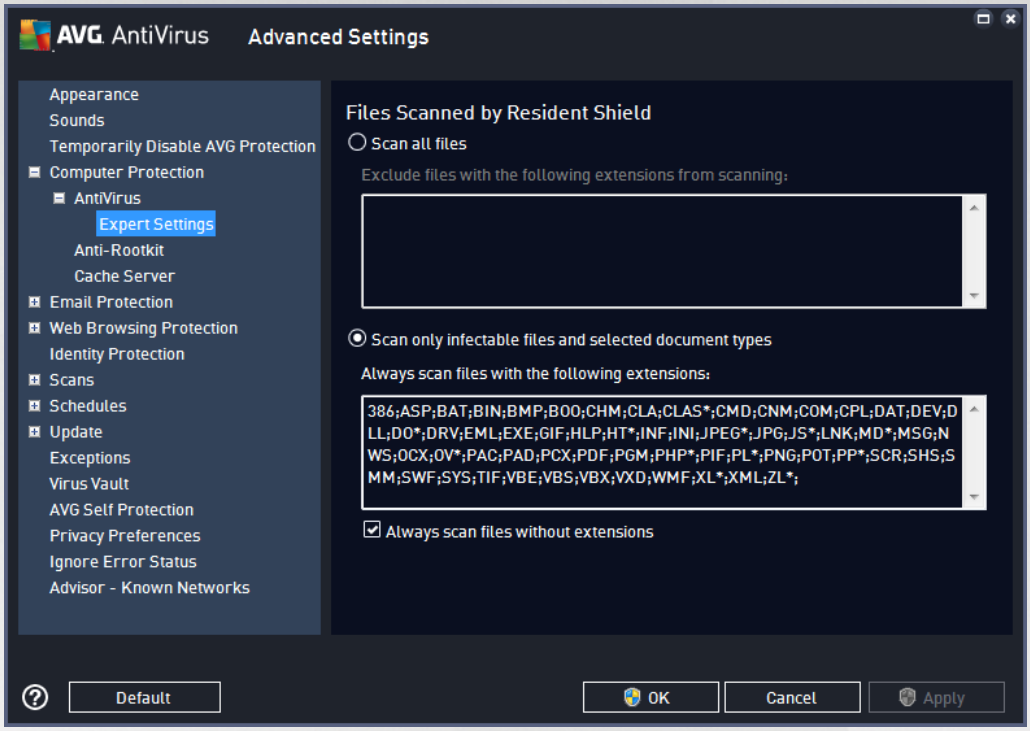
- ***Use Heuristics*** (*on by default*) - heuristic analysis will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*).

- ***Scan files referred in registry*** (*on by default*) - this parameter defines that AVG will scan all executable files added to the startup registry to avoid a known infection being executed upon next computer startup.

- ***Enable thorough scanning*** (*off by default*) - in specific situations (*in a state of extreme emergency*) you may check this option to activate the most thorough algorithms that will check all possibly threatening objects in-depth. Remember though that this method is rather time consuming.

- ***Enable Instant Messaging protection and P2P download protection*** (*on by default*) - check this item if you wish to verify that the instant messaging communication (*e.g. AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) and data downloaded within Peer-to-Peer networks *(networks allowing direct connection between clients, without a server, which is potentially dangerous; typically used to share music files)* are virus free.

In the ***Files Scanned by the Resident Shield*** dialog it is possible to configure which files will be scanned (*by specific extensions*):

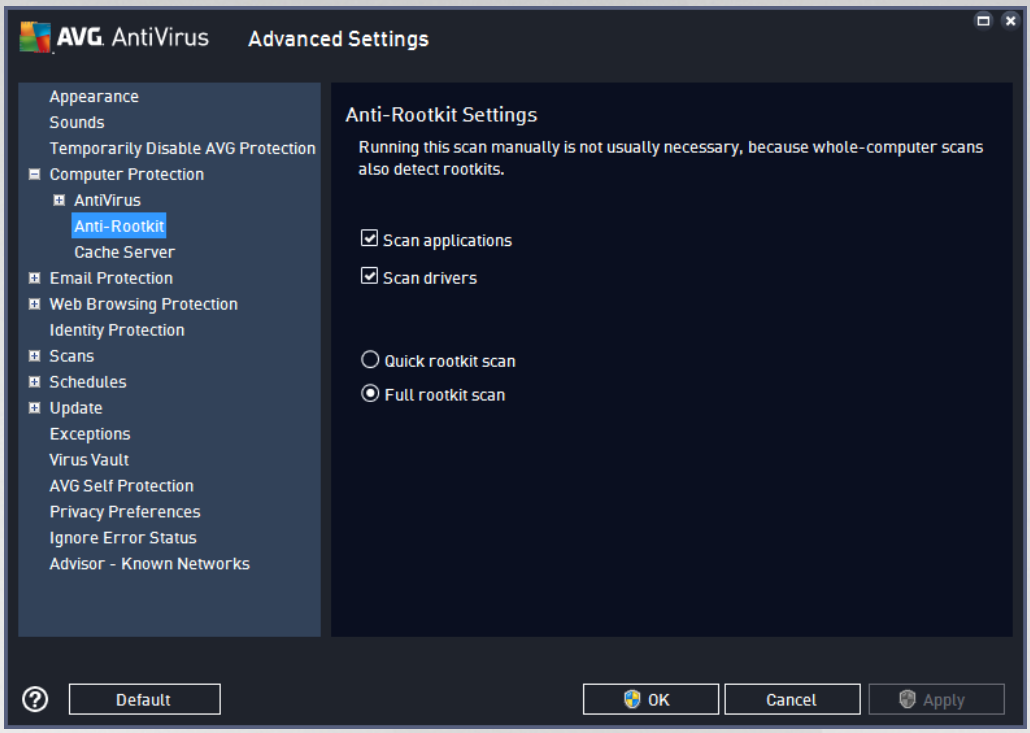


Mark the respective checkbox to decide whether you want to ***Scan all files*** or ***Scan infectable files and selected types of documents*** only. To speed up the scanning and provide the maximum level of protection at the same time, we recommend that you keep the default settings. This way only infectable files will be scanned. In the respective section of the dialog you can also find an editable a list of extensions defining files that are included in scanning.

Check the ***Always scan files without extensions*** (*on by default*) to ensure that even files with no extension and unknown format should be scanned by the Resident Shield. We recommend that you keep this feature switched on, as files without extensions are suspicious.

7.4.2. Anti-Rootkit

In the ***Anti-Rootkit Settings*** dialog you can edit the ***Anti-Rootkit*** service configuration and specific parameters of anti-rootkit scanning. The anti-rootkit scanning is a default process included in the Whole Computer Scan:

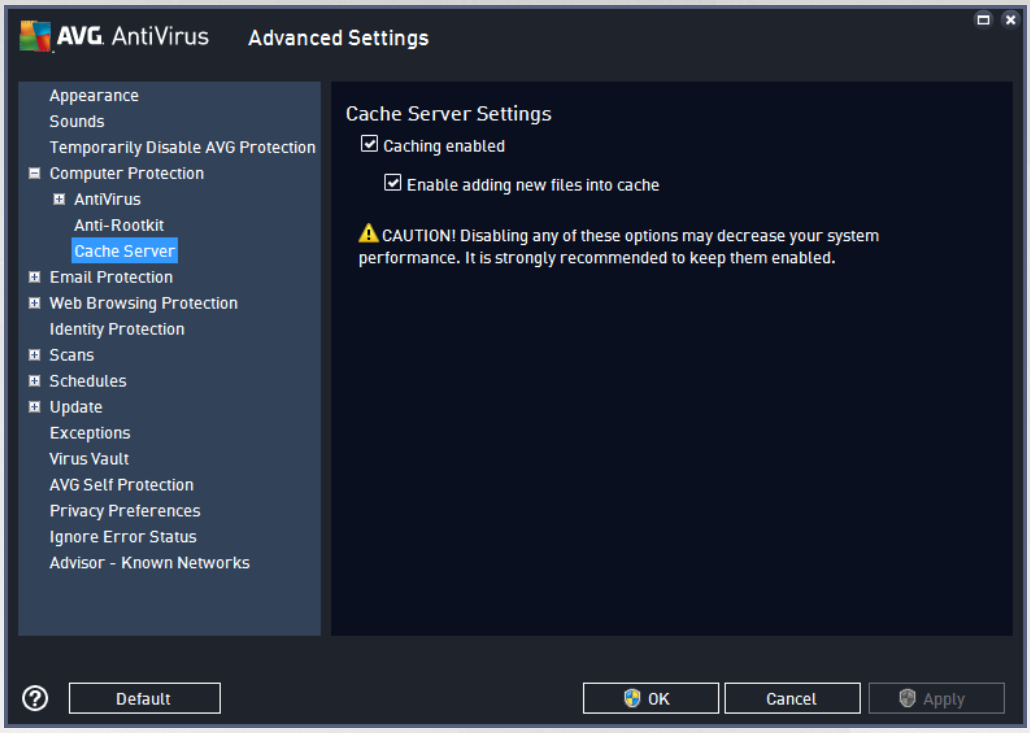


Scan applications and ***Scan drivers*** enable you to specify in detail what should be included in anti-rootkit scanning. These settings are intended for advanced users; we recommend that you keep all options switched on. You can also pick the rootkit scanning mode:

- ***Quick rootkit scan*** - scans all running processes, loaded drivers and the system folder (*typically c:\Windows*)
- ***Full rootkit scan*** - scans all running processes, loaded drivers, the system folder (*typically c:\Windows*), plus all local disks (*including the flash disk, but excluding floppy disk/CD drives*)

7.4.3. Cache Server

The ***Cache Server Settings*** dialog refers to the cache server process designed to speed up all types of **AVG AntiVirus 2015** scans:



The cache server gathers and keeps information on trustworthy files (*a files is considered trustworthy if signed with digital signature on a trustworthy source*). These files are then automatically considered to be safe, and do not need to be re-scanned; therefore these files are skipped during scanning.

The ***Cache Server Settings*** dialog offers the following options for configuration:

- ***Caching enabled*** (*on by default*) - uncheck the box to switch off the ***Cache Server***, and empty the cache memory. Please note that scanning might slow down, and overall performance of your computer decrease, as every single file in use will be scanned for viruses and spyware first.
- ***Enable adding new files into cache*** (*on by default*) - uncheck the box to stop adding more files into the cache memory. Any already cached files will be kept and used until caching is turned off completely, or until the next update of the virus database.

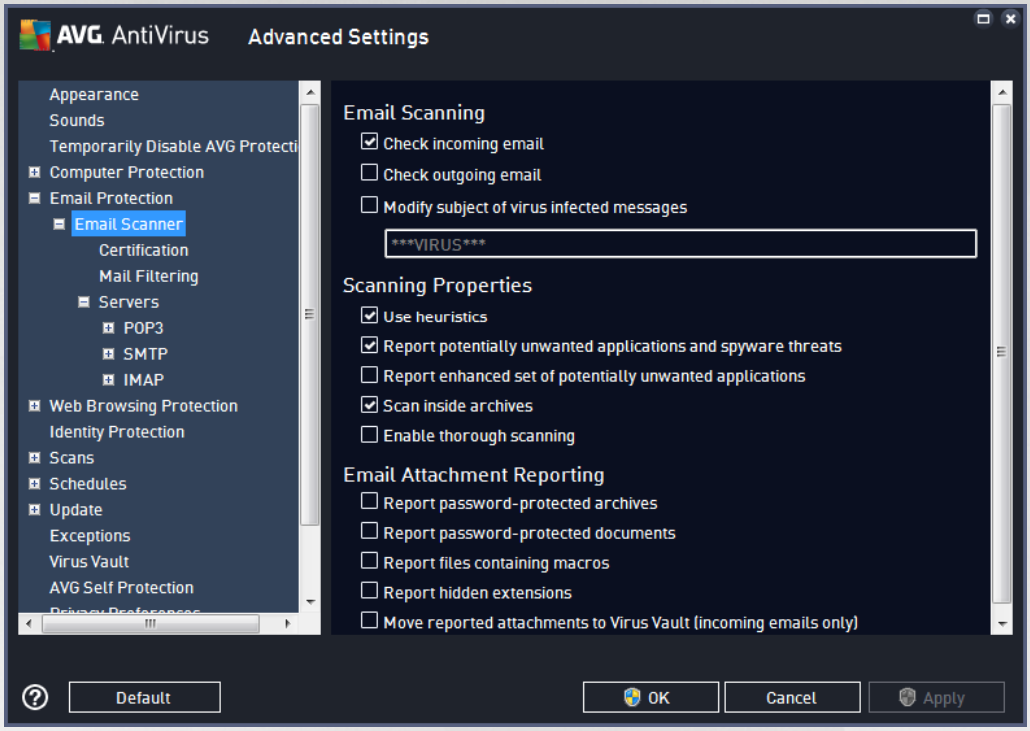
Unless you have a good reason to switch the cache server off, we strongly recommend that you keep the default settings and leave both the options on! Otherwise you may experience a significant decrease in your system speed and performance.

7.5. Email Scanner

In this section you can edit the detailed configuration of Email Scanner and Anti-Spam:

7.5.1. Email Scanner

The ***Email Scanner*** dialog is divided into three sections:



Email scanning

In this section, you can set these basics for incoming and/or outgoing email messages:

- ***Check incoming email*** (*on by default*) - mark to switch on/off the option of scanning of all email messages delivered to your email client
- ***Check outgoing email*** (*off by default*) - mark to switch on/off the option of scanning of all emails sent from your account
- ***Modify subject of virus infected messages*** (*off by default*) - if you want to be warned that the scanned email message was detected as infected, mark this item and fill in the desired text into the text field. This text will then be added to the "Subject" field for each detected email message for easier identification and filtering. The default value is ***VIRUS*** which we recommend that you keep.

Scanning properties

In this section, you can specify how the email messages will be scanned:

- ***Use Heuristics*** (*on by default*) - check to use the heuristics detection method when scanning email messages. When this option is on, you can filter email attachments not only by the extension but the actual contents of the attachment will also be considered. The filtering can be set in the Mail Filtering dialog.

- ***Report Potentially Unwanted Applications and Spyware threats*** (*on by default*) - check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of Potentially Unwanted Applications*** (*off by default*) - mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan inside archives*** (*on by default*) - check to scan contents of archives attached to email messages.

- ***Enable thorough scanning*** (*off by default*) - in specific situations (*e.g. suspicions of your computer being infected by an virus or attack*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that hardly ever get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

Email attachments reporting

In this section, you can set additional reports about potentially dangerous or suspicious files. Please note that no warning dialog will be displayed; a certification text will only be added to the end of the email message, and all such reports will be listed in the Email Protection detection dialog:

- ***Report password protected archives*** - archives (*ZIP, RAR etc.*) that are protected by password cannot be scanned for viruses; check the box to report these as potentially dangerous.

- ***Report password protected documents*** - documents protected by password cannot be scanned for viruses; check the box to report these as potentially dangerous.

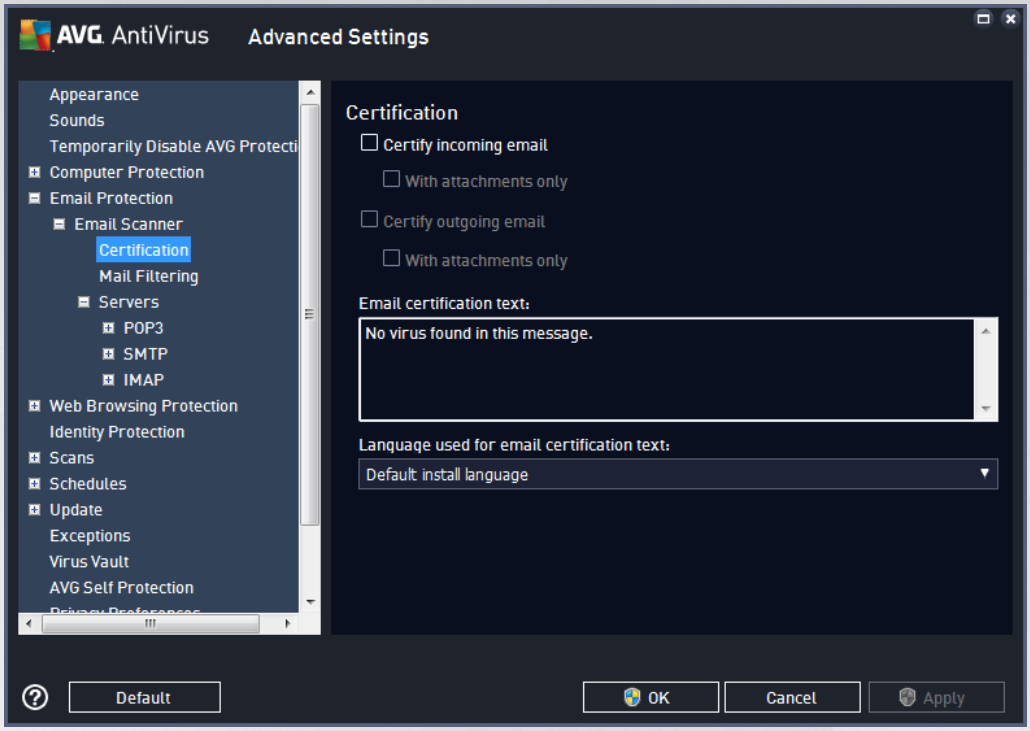
- ***Report files containing macro*** - a macro is a predefined sequence of steps aimed to make certain tasks easier for a user (*MS Word macros are widely known*). As such, a macro can contain potentially dangerous instructions, and you might like to check the box to ensure that files with macros will be reported as suspicious.

- ***Report hidden extensions*** - a hidden extension can make e.g. a suspicious executable file "something.txt.exe" appear as harmless plain text file "something.txt"; check the box to report these as potentially dangerous.

- ***Move reported attachments to Virus Vault*** - specify whether you wish to be notified via email about password protected archives, password protected documents, files containing macros, and/or files with hidden extensions detected as an attachment to the scanned email message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the Virus Vault.

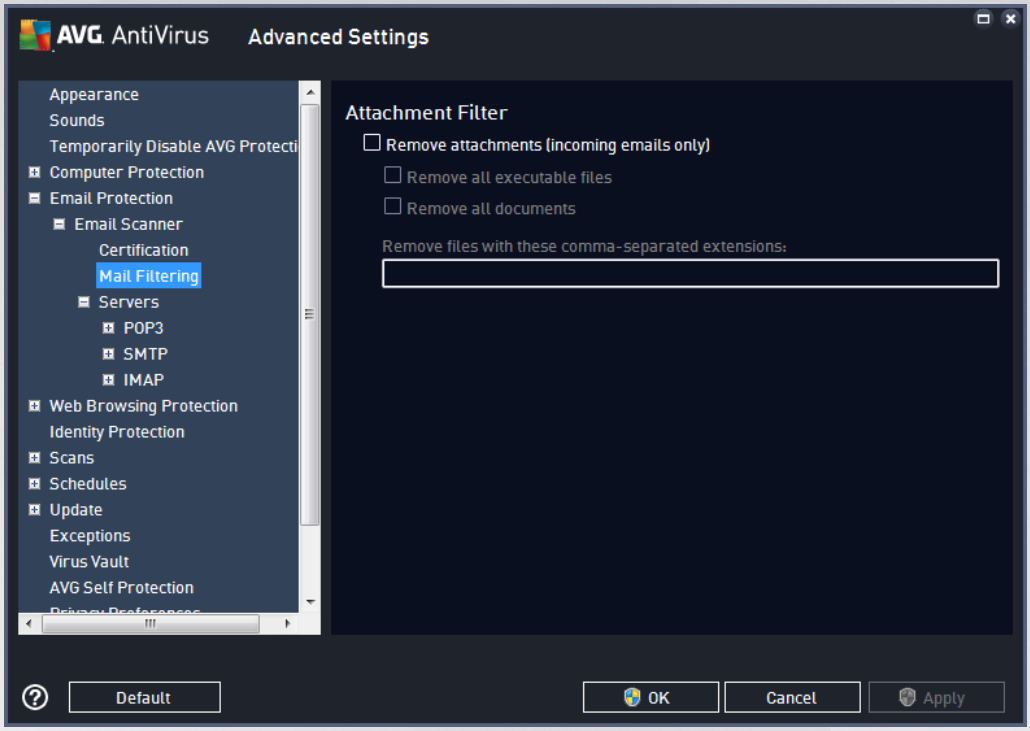
In the ***Certification*** dialog you can mark the specific checkboxes to decide whether you want to certify your incoming mail (***Certify incoming email***) and/or outgoing mail (***Certify outgoing email***). For each of these options you can further specify the ***With attachments only*** parameter so that the certification is only added to

email messages with attachments:



By default, the certification text consists of just a basic information that states *No virus found in this message.* However, this information can be extended or changed according to your needs: write the desired text of certification into the ***Email certification text*** field. In the ***Language used for the email certification text*** section you can further define in which language the automatically generated part of the certification (*No virus found in this message*) should be displayed.

Note: *Please bear in mind that only the default text will be displayed in the requested language, and your customized text will not be translated automatically!*



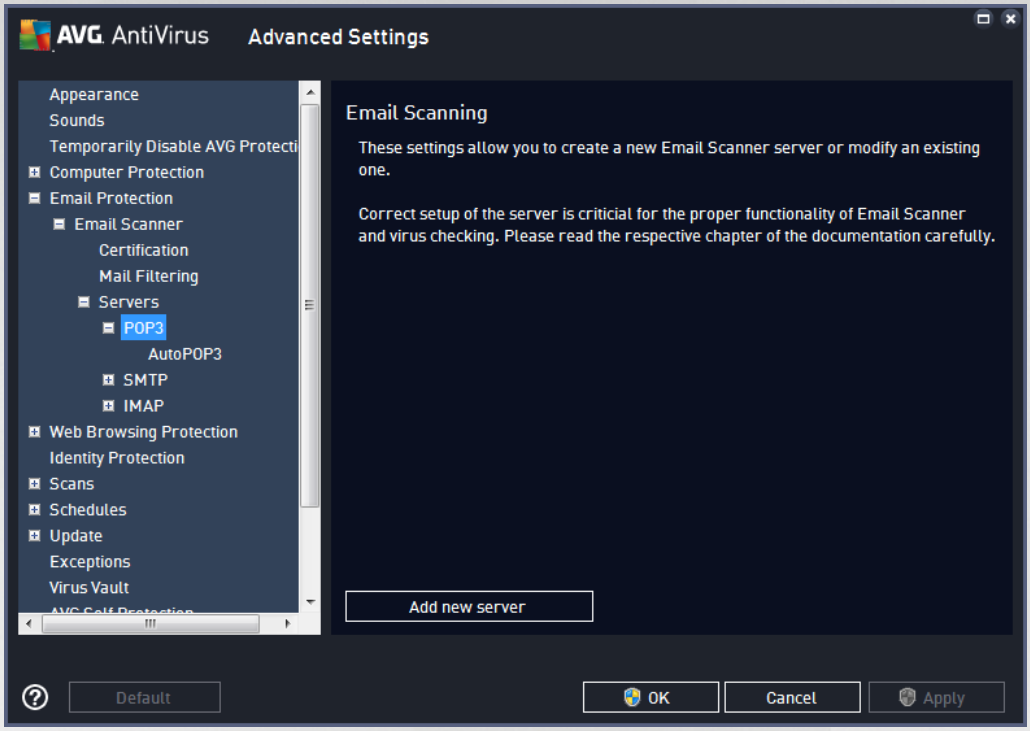
The ***Attachment filter*** dialog allows you to set up parameters for email message attachment scanning. By default, the ***Remove attachments*** option is switched off. If you decide to activate it, all email message attachments detected as infected or potentially dangerous will be removed automatically. If you want to define specific types of attachments that should be removed, select the respective option:

- ***Remove all executable files*** - all *.exe files will be deleted
- ***Remove all documents*** - all *.doc, *.docx, *.xls, *.xlsx files will be deleted
- ***Remove files with these comma separated extensions*** - will remove all files with the defined extensions

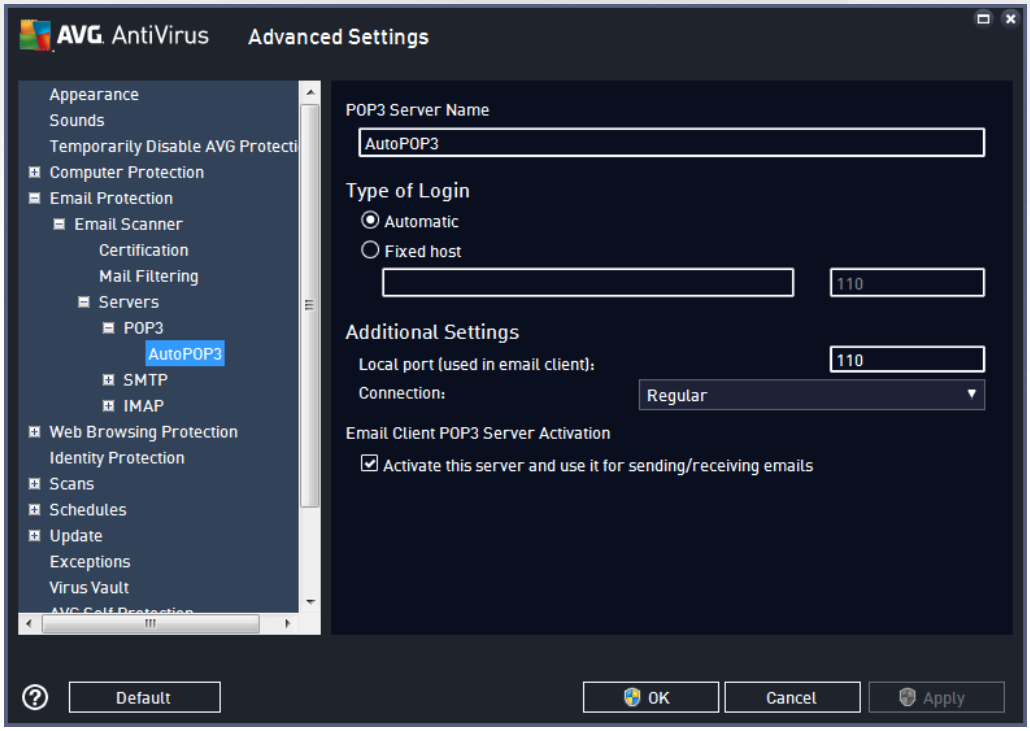
In the ***Servers*** section you can edit parameters for the Email Scanner servers:

- POP3 server
- SMTP server
- IMAP server

You can also define new servers for incoming or outgoing mail, using the ***Add new server*** button.

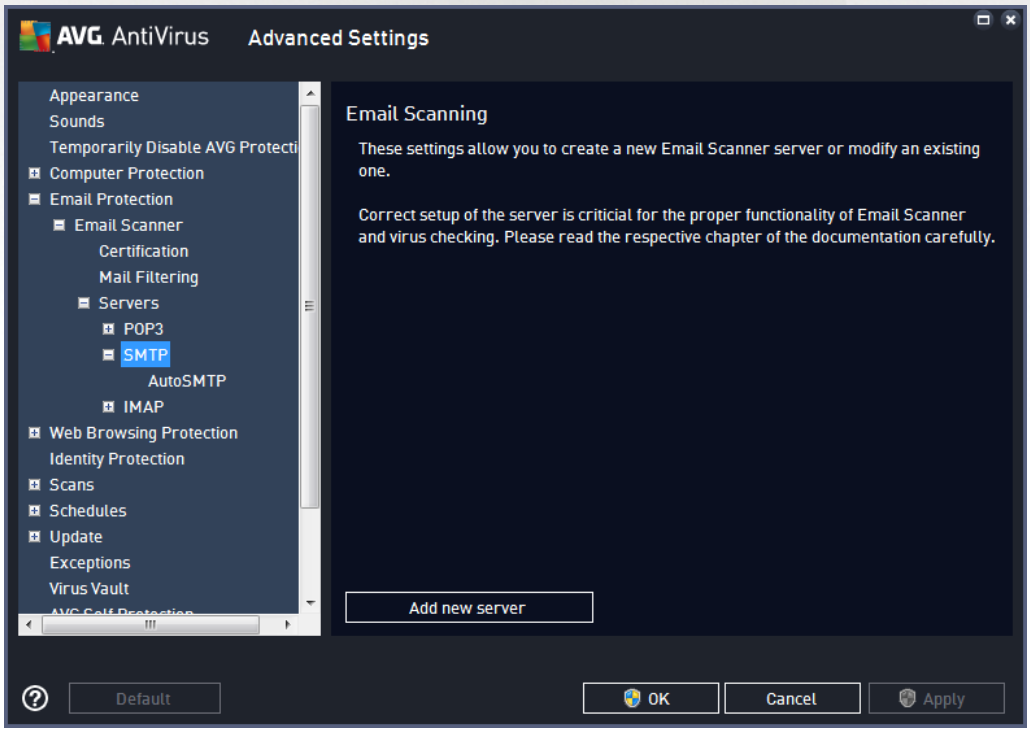


In this dialog you can set up a new Email Scanner server using the POP3 protocol for incoming mail:

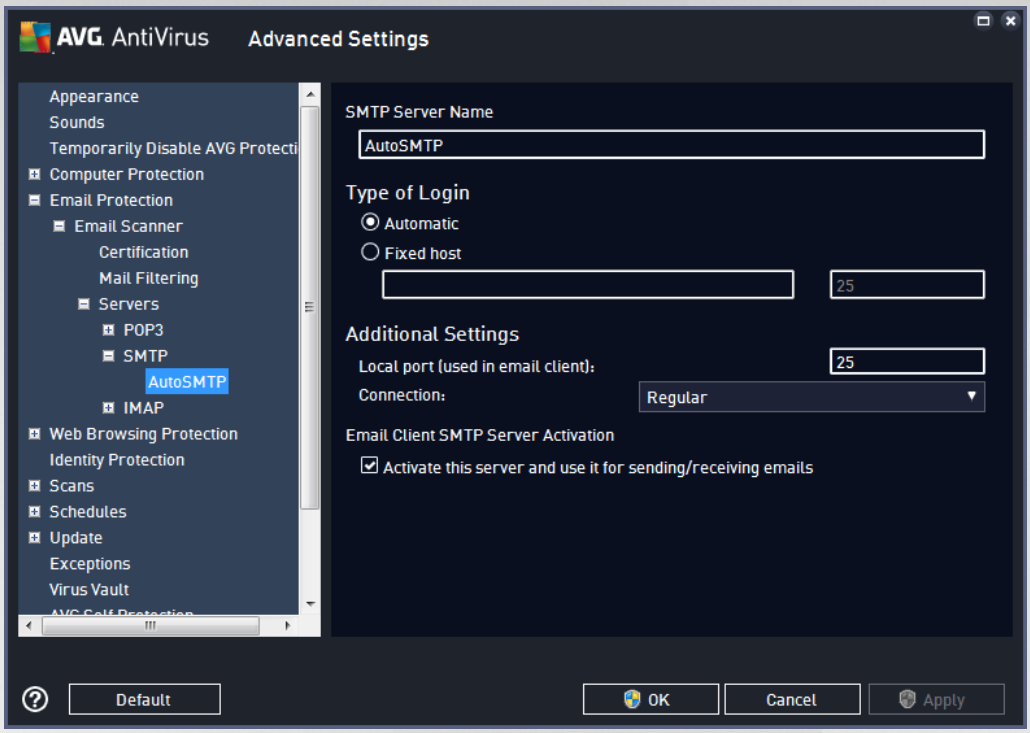


- ***POP3 Server Name*** - in this field you can specify the name of newly added servers (*to add a POP3 server, click the right mouse button over the POP3 item of the left navigation menu*).

- ***Type of Login*** - defines the method for determining the mail server used for incoming mail:
    - o ***Automatic*** - login will be carried out automatically, according to your email client settings.
    - o ***Fixed host*** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. The login name remains unchanged. For a name, you may use a domain name (*for example, pop.acme.com*) as well as an IP address (*for example, 123.45.67.89*). If the mail server uses a non-standard port, you can specify this port after the server name using a colon as the delimiter (*for example, pop.acme.com:8200*). The standard port for POP3 communication is 110.
- ***Additional Settings*** - specifies more detailed parameters:
    - o ***Local port*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for POP3 communication.
    - o ***Connection*** - in the drop-down menu, you can specify which kind of connection to use (*regular/ SSL/SSL default*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- ***Email Client POP3 Server Activation*** - check/uncheck this item to activate or deactivate the specified POP3 server



In this dialog you can set up a new Email Scanner server using the SMTP protocol for outgoing mail:



- ***SMTP Server Name*** - in this field you can specify the name of newly added servers (*to add a SMTP server, click the right mouse button over the SMTP item of the left navigation menu*). For automatically created "AutoSMTP" servers this field is deactivated.

- ***Type of Login*** - defines the method for determining the mail server used for outgoing mail:

  - ***Automatic*** - login will be carried out automatically, according to your email client settings

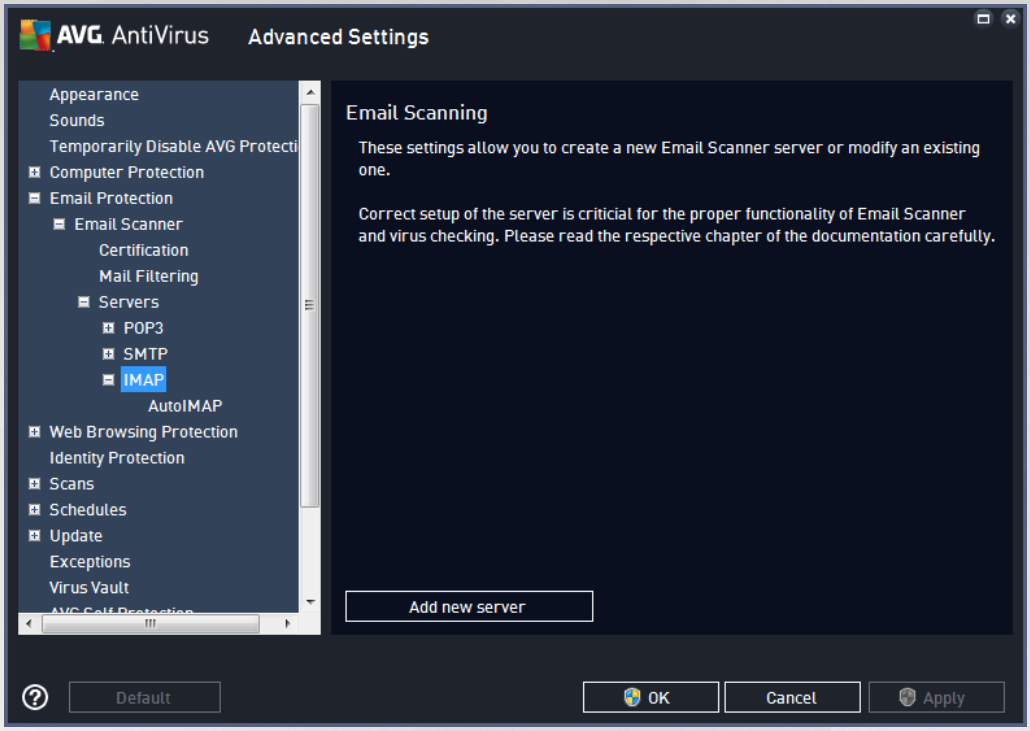
  - ***Fixed host*** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (*for example, smtp.acme.com*) as well as an IP address (*for example, 123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (*for example, smtp.acme.com:8200*). The standard port for SMTP communication is 25.

- ***Additional Settings*** - specifies more detailed parameters:

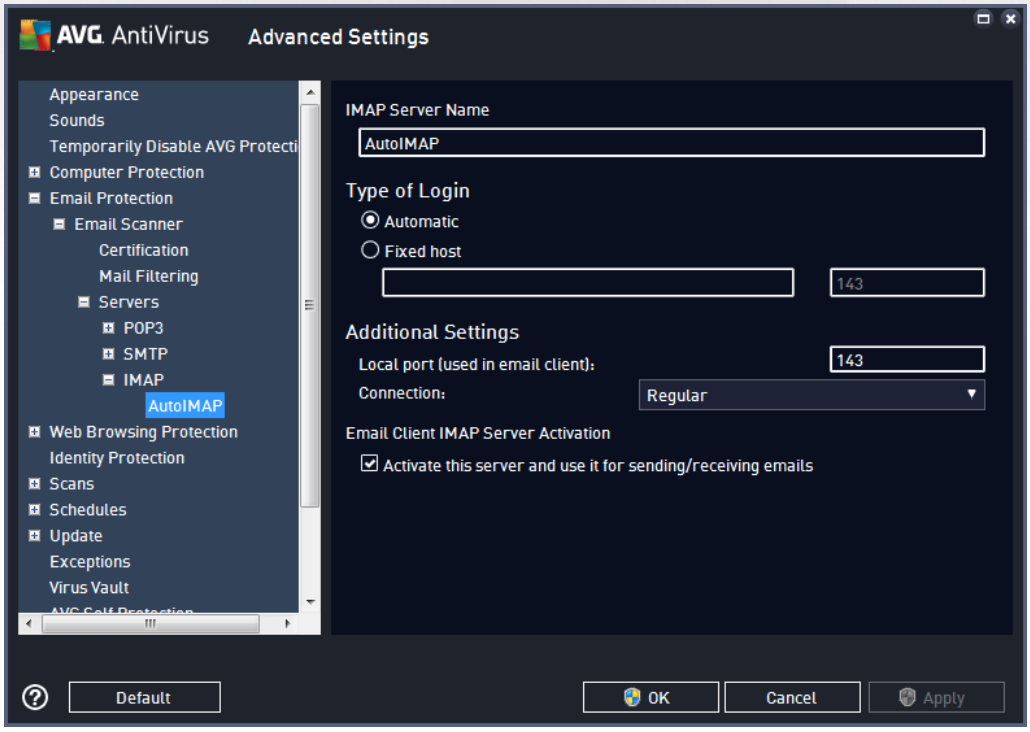
  - ***Local port*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for SMTP communication.

  - ***Connection*** - in this drop-down menu, you can specify which kind of connection to use (*regular/SSL/SSL default*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.

- ***Email Client SMTP Server Activation*** - check/uncheck this box to activate/deactivate the SMTP server specified above



In this dialog you can set up a new Email Scanner server using the IMAP protocol for outgoing mail:

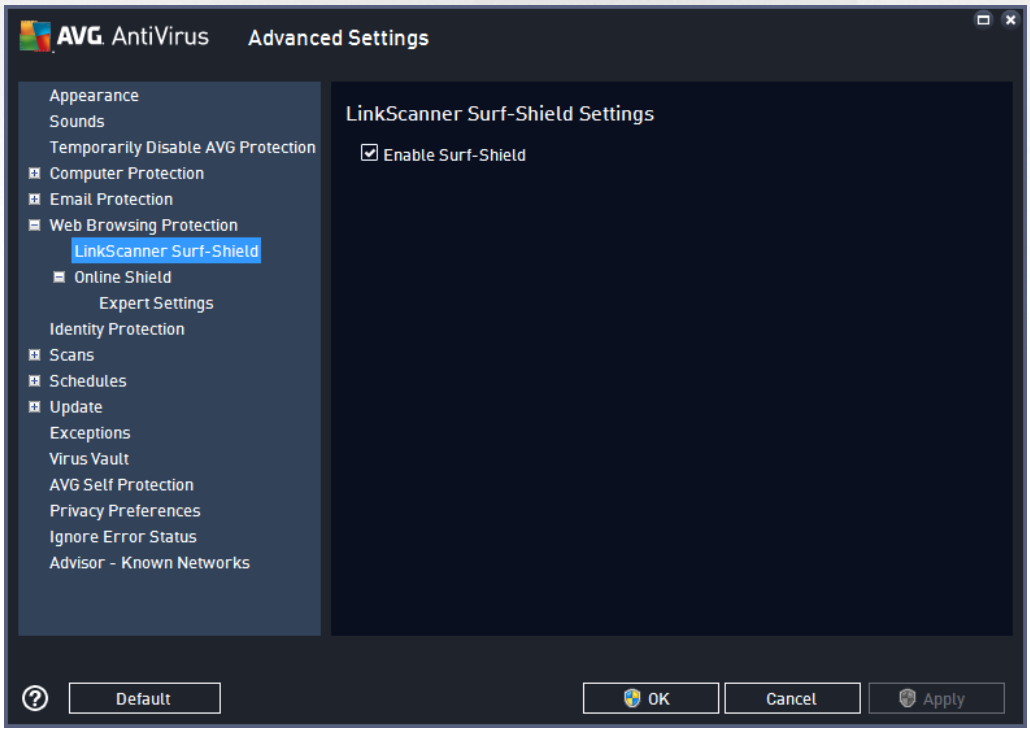


- ***IMAP Server Name*** - in this field you can specify the name of newly added servers (*to add a IMAP server, click the right mouse button over the IMAP item of the left navigation menu*).

- ***Type of Login*** - defines the method for determining the mail server used for outgoing mail:
    - o ***Automatic*** - login will be carried out automatically, according to your email client settings
    - o ***Fixed host*** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (*for example, smtp.acme.com*) as well as an IP address (*for example, 123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (*for example, imap.acme.com:8200*). The standard port for IMAP communication is 143.
- ***Additional Settings*** - specifies more detailed parameters:
    - o ***Local port used in*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for IMAP communication.
    - o ***Connection*** - in this drop-down menu, you can specify which kind of connection to use (*regular/SSL/SSL default*). If you choose a SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.
- ***Email client IMAP Server Activation*** - check/uncheck this box to activate/deactivate the IMAP server specified above

7.6. Web Browsing Protection

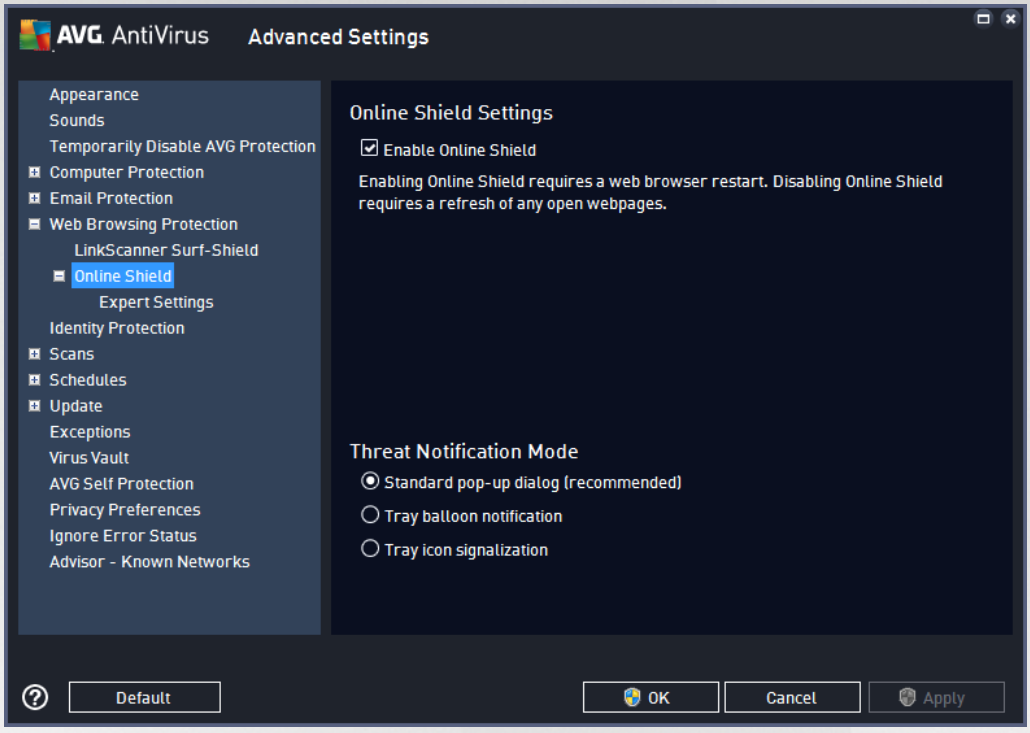
The ***LinkScanner settings*** dialog allows you to check/uncheck the following features:



- ***Enable Surf-Shield*** - (*on by default*): active (*real-time*) protection against exploitative sites as they

are accessed. Known malicious site connections and their exploitative content are blocked as they are accessed by the user via a web browser (*or any other application that uses HTTP*).

7.6.1. Online Shield

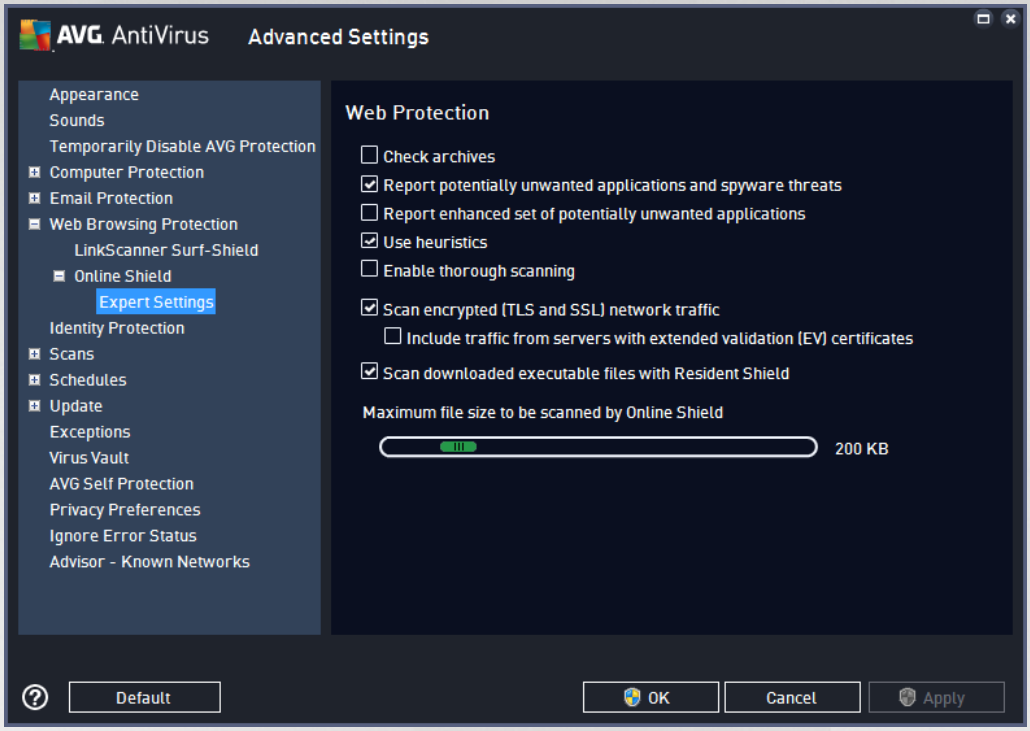


The ***Online Shield*** dialog offers the following options:

- ***Enable Online Shield*** *(on, by default)* - Activate/deactivate the entire ***Online Shield*** service. For further advanced settings of ***Online Shield*** please continue to the subsequent dialog called Web Protection.

Threat notification mode

In the bottom section of the dialog, select the method by which you wish to be informed about a potential detected threat: via standard pop-up dialog, via tray balloon notification, or via tray icon info.



In the ***Web Protection*** dialog you can edit the component's configuration regarding the scan of the website content. The editing interface allows you to configure the following elementary options:

- ***Check archives*** - (*off by default*): scan the content of archives possibly included in the www page to be displayed.
- ***Report potentially unwanted applications and spyware threats*** - (*on by default*): check to activate the scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.
- ***Report enhanced set of potentially unwanted applications*** - (*off by default*): mark to detect extended package of spyware: programs that are perfectly OK and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.
- ***Use heuristics*** - (*on by default*): scan the content of the page to be displayed using the heuristic analysis method (*dynamic emulation of the scanned object's instructions in a virtual computer environment*).
- ***Enable thorough scanning*** - (*off by default*): in specific situations (*suspicions about your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.
- ***Scan encrypted (TLS and SSL) network traffic*** - (*on by default*): leave marked to allow AVG

scan also all encrypted network communication, that is, connections over security protocols (SSL and its newer version, TLS). This applies to websites using HTTPS, and email client connections using TLS/SSL. The secured traffic is decrypted, scanned for malware, and encrypted again to be delivered safely to your computer. Within this option you can decide to ***Include traffic from servers with extended validation (EV) certificates*** and scan also encrypted network communication from servers certified with Extended Validation Certificate. Issuing an EV certificate requires extensive validation by the certificate authority, and websites operated under the certificate are therefore much more trustworthy *(less likely to distribute malware)*. For this reason, you may decide not to scan traffic from EV certified servers, which will make the encrypted communication moderately faster.

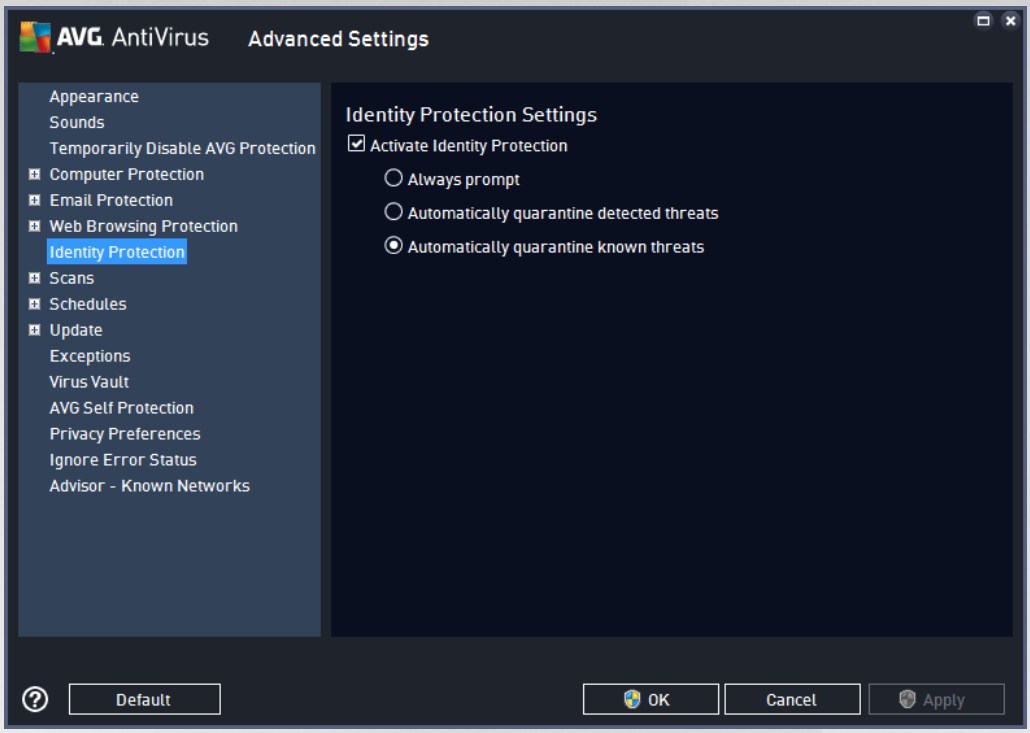
- ***Scan downloaded executable files with Resident Shield*** - (*on by default*): scan executable files *(typically files with extensions exe, bat, com)* after they have been downloaded. The resident shield scans files before download to ensure no malicious code gets into your computer. However, this scanning is limited by the ***Maximum part size of file to be scanned*** - see the next item in this dialog. Therefore large files are scanned part-by-part, and this is also true for most executable files. Executable files can perform various tasks in your computer, and it is vital that they are 100% safe. This can be ensured by both scanning the file in parts before it is downloaded, and also right after the file download is completed. We recommend that you keep this option checked. If you deactivate this option, you can still rest assured that AVG will find any potentially dangerous code. Only usually it will not be able to evaluate an executable file as a complex, so it might produce some false positives.

The slider down in the dialog allows you to define ***Maximum part size of a file to be scanned*** - if included files are present in the displayed page you can also scan their content even before these are downloaded to your computer. However, scanning of large files takes quite some time and the web page download might be slowed significantly. You can use the slide bar to specify the maximum size of a file that is still to be scanned with ***Online Shield***. Even if the downloaded file is bigger than specified, and therefore will not be scanned with Online Shield, you are still protected: if the file is infected, the ***Resident Shield*** will detect it immediately.

7.7. Identity Protection

Identity Protection is an anti-malware component that protects you from all kinds of malware (*spyware, bots, identity theft, ...*) using behavioral technologies and provides zero day protection for new viruses *(for a detailed description of the component's functionality please consult the Identity chapter*).

The ***Identity Protection settings*** dialog allows you to switch the elementary features of the Identity Protection component on/off:



Activate Identity Protection (*on by default*) - uncheck to turn off the Identity component. ***We strongly recommend not doing this unless you have to!*** When the Identity Protection is activated, you can specify what to do when a threat is detected:

- ***Always prompt*** - when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- ***Automatically quarantine detected threats*** - mark this checkbox to specify that you want to have all possibly detected threats moved to the safe space of the Virus Vault immediately. Keeping the default settings, when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- ***Automatically quarantine known threats*** (*on by default*) - keep this item marked if you wish all applications detected as possible malware to be automatically and immediately moved to the Virus Vault.

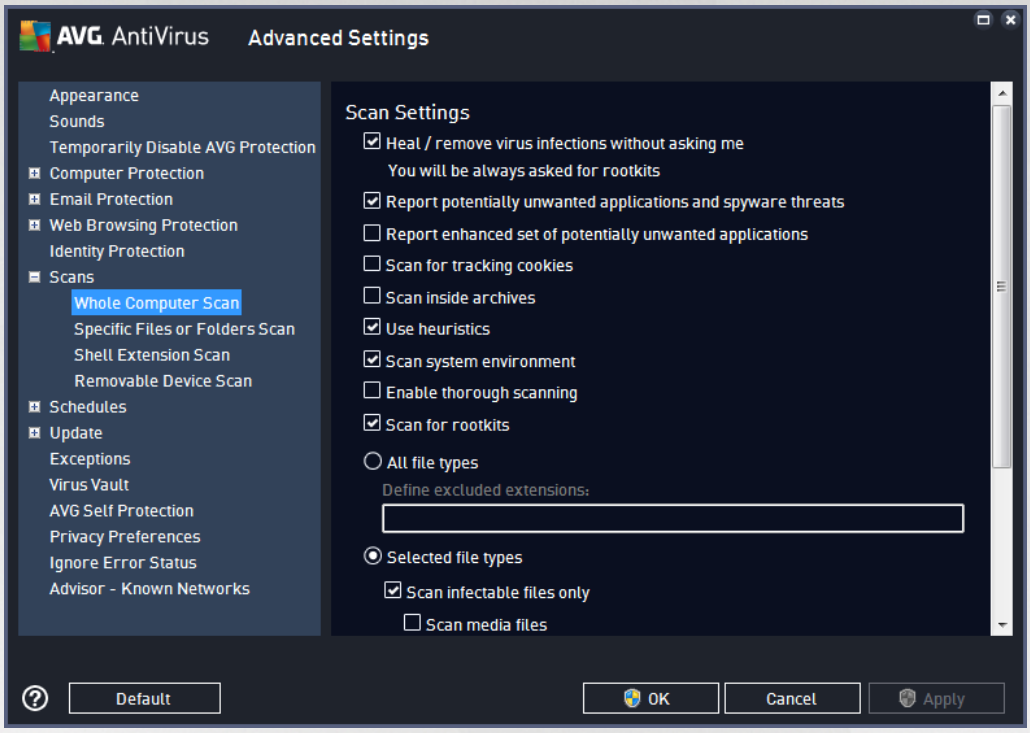
7.8. Scans

The advanced scan settings are divided into four categories referring to specific scan types as defined by the software vendor:

- Whole computer scan - standard predefined scan of the entire computer
- Specific files or folders scan - standard predefined scan of selected areas of your computer
- Shell extension scan - specific scanning of a selected object directly from the Windows Explorer environment
- Removable device scan - specific scanning of removable devices attached to your computer

7.8.1. Whole Computer Scan

The ***Whole Computer Scan*** option allows you to edit parameters of one of the scans predefined by the software vendor, Whole Computer Scan:



Scan settings

The ***Scan Settings*** section offers a list of scanning parameters that can be optionally switched on/off:

- ***Heal / remove virus infection without asking me*** (*on by default*) - if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.
- ***Report potentially unwanted applications and spyware threats*** (*on by default*) - check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.
- ***Report enhanced set of potentially unwanted applications*** (*off by default*) - mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.
- ***Scan for tracking cookies*** (*off by default*) - this parameter stipulates that cookies should be detected; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*).

- ***Scan inside archives*** (*off by default*) - this parameter stipulates that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...
- ***Use heuristics*** (*on by default*) - heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning.
- ***Scan system environment*** (*on by default*) - scanning will also check the system areas of your computer.
- ***Enable thorough scanning*** (*off by default*) - in specific situations (*suspicions about your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.
- ***Scan for rootkits*** (*on by default*) - Anti-Rootkit scan searches your PC for possible rootkits, i.e. programs and technologies that can cover malware activity in your computer. If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

You should also decide whether you want to scan

- ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated (*after being saved, the commas change into semicolons*) file extensions that should not be scanned.
- ***Selected file types*** - you can specify that you want to scan only files that can be infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.
- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

Adjust how quickly scan completes

Within the ***Adjust how quickly scan completes*** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to *user sensitive* level of automatic resource usage. If you want the scanning to run faster, it will take less time but the system resources used will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease system resources used by extending the scanning duration.

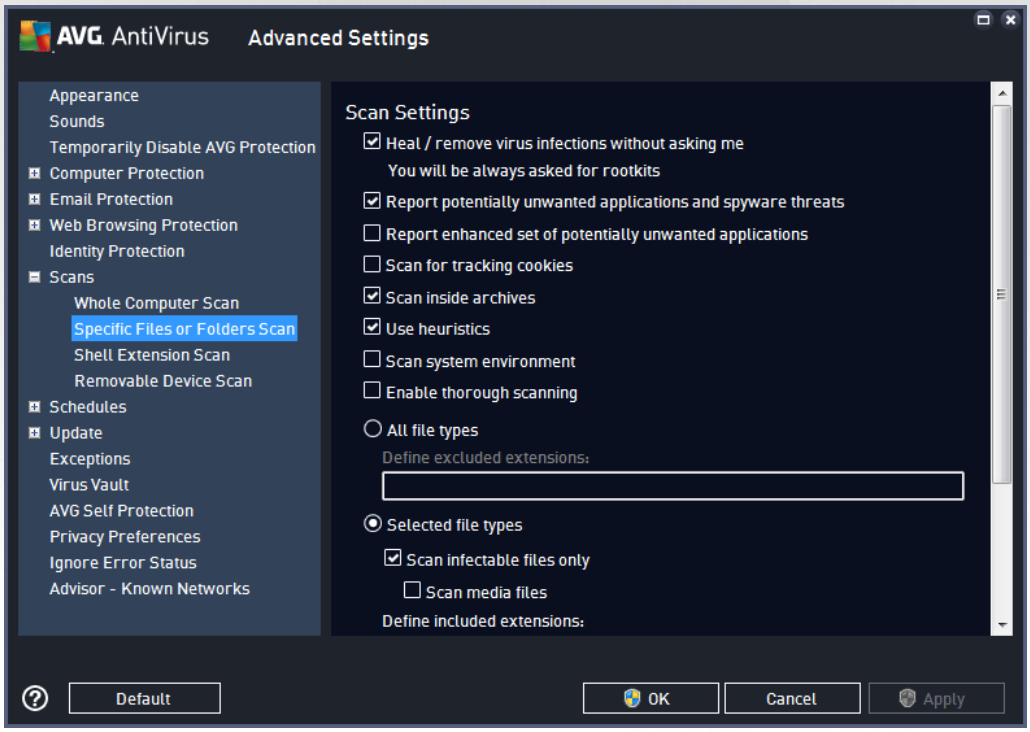
Set additional scan reports ...

Click the ***Set additional scan reports ...*** link to open a standalone dialog window called ***Scan reports*** where you can tick several items to define what scan findings should be reported:



7.8.2. Specific Files or Folders Scan

The editing interface for ***Scan Specific Files or Folders*** is almost identical to the Whole Computer Scan editing dialog, however the default settings are more strict for the Scan of the Whole Computer:

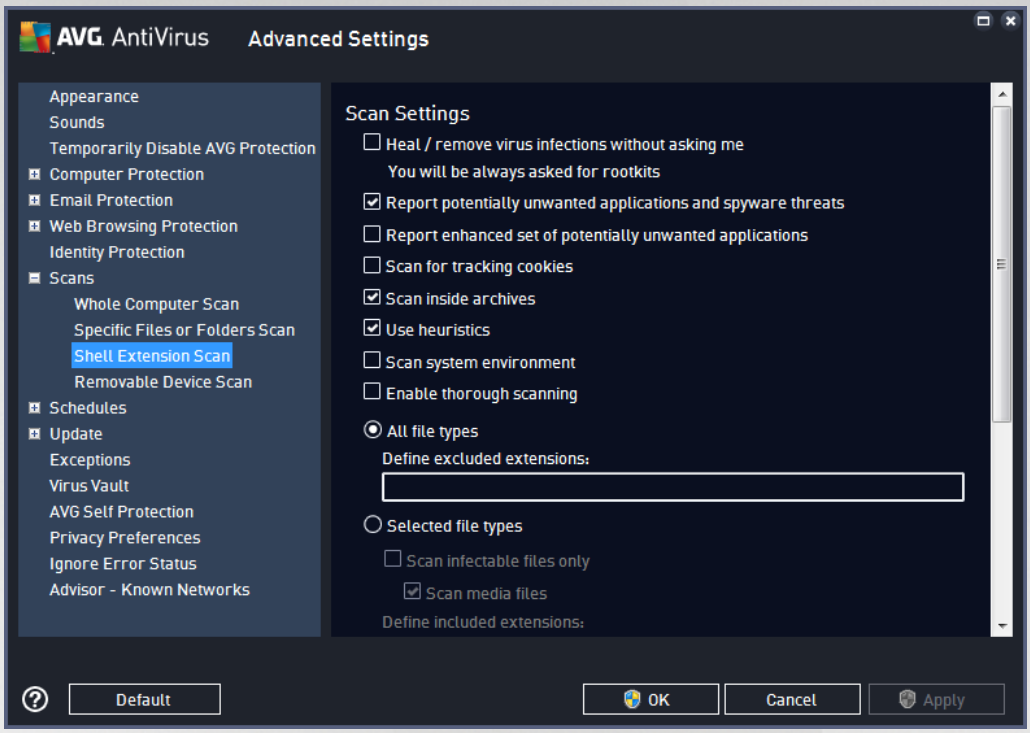


All parameters set up in this configuration dialog apply only to the areas selected for scanning with Scan of Specific Files or Folders!

Note: *For a description of specific parameters please consult the AVG Advanced Settings / Scans / Whole Computer Scan chapter.*

7.8.3. Shell Extension Scan

Similar to the previous Whole Computer Scan item, this item named ***Shell Extension Scan*** also offers several options for editing the scan predefined by the software vendor. This time the configuration is related to scanning of specific objects launched directly from the Windows Explorer environment (*shell extension*), see Scanning in Windows Explorer chapter:



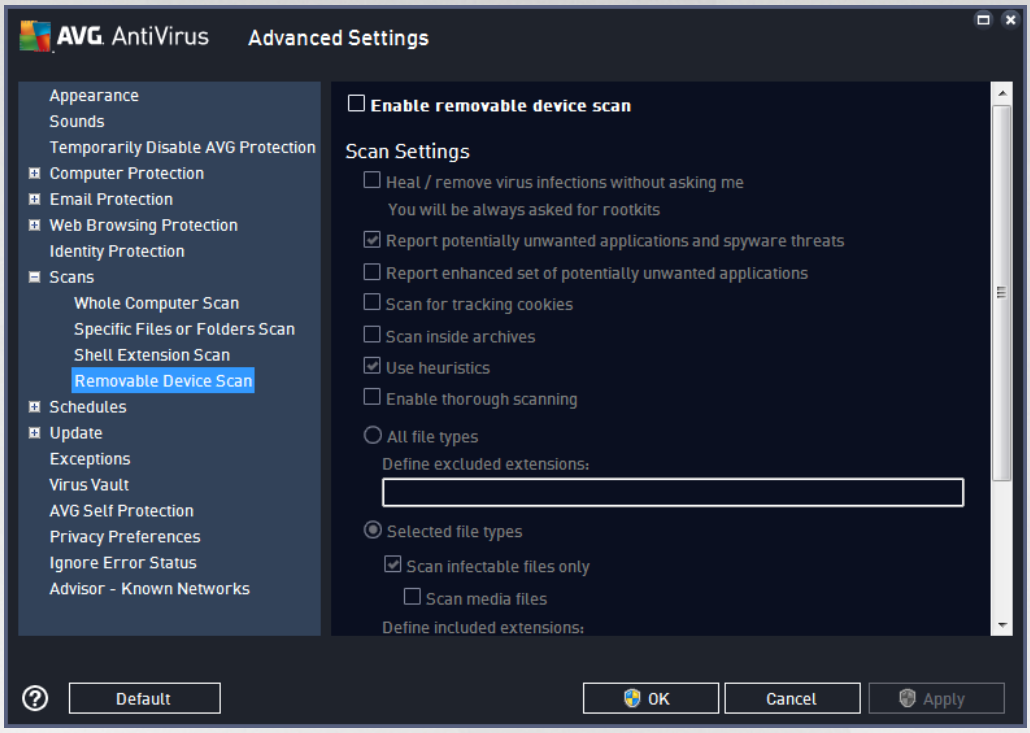
The editing options are almost identical to those available for the Scan of the Whole Computer, however, the default settings differ (*for instance, Whole Computer Scan by default does not check the archives but it does scan the system environment; vice versa with the Shell Extension Scan*).

Note: *For a description of specific parameters please consult the AVG Advanced Settings / Scans / Whole Computer Scan chapter.*

Compared to the Whole Computer scan dialog, the ***Shell Extension Scan*** dialog also includes the section named ***Displaying of scan progress and results***, where you can specify whether you want the scan progress and scan results to be accessible from the AVG user interface. You can also specify that the scan result should only be displayed in case an infection is detected during scanning.

7.8.4. Removable Device Scan

The editing interface for ***Removable Device Scan*** is also very similar to the Whole Computer Scan editing dialog:



The ***Removable Device Scan*** is launched automatically once you attach any removable device to your computer. By default, this scan is switched off. However, it is crucial to scan removable devices for potential threats since these are a major source of infection. To have this scan ready and launched automatically when needed, mark the ***Enable Removable device scan*** option.

Note: *For a description of specific parameters please consult the AVG Advanced Settings / Scans / Whole Computer Scan chapter.*

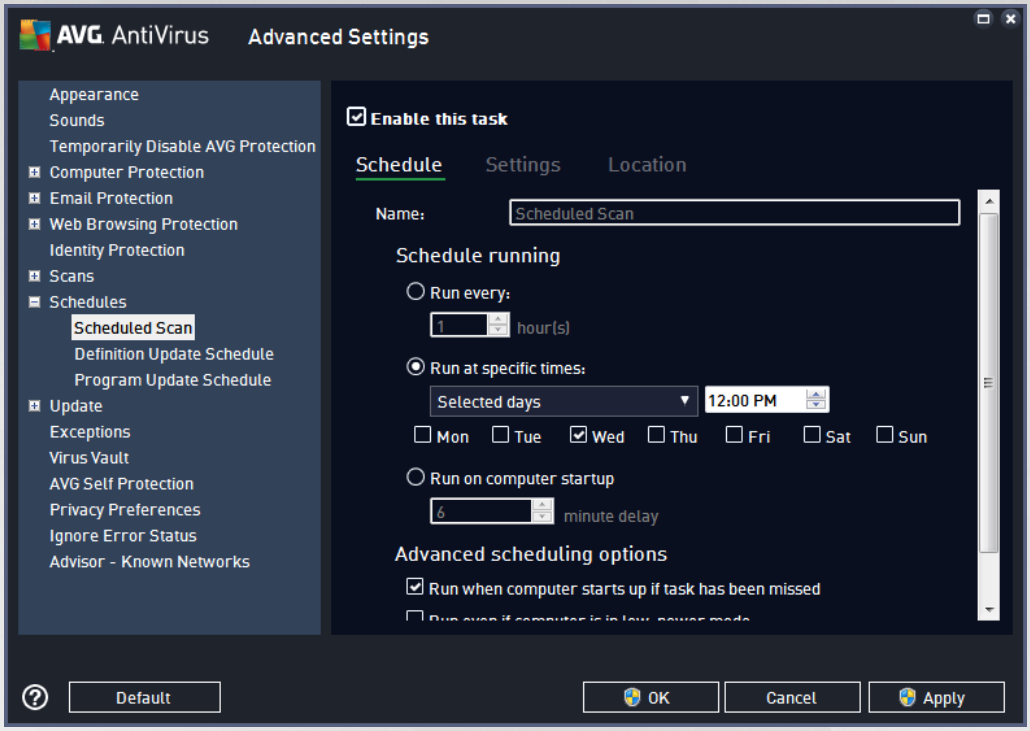
7.9. Schedules

In the ***Schedules*** section you can edit the default settings of:

- Scheduled Scan
- Definitions Update Schedule
- Program Update Schedule

7.9.1. Scheduled Scan

The parameters of the scheduled scan can be edited (*or a new schedule set up*) on three tabs. On each tab you can first check/uncheck the ***Enable this task*** item to simply deactivate the scheduled test temporarily, and switch it on again as the need arises:



Next, the text field called ***Name*** (*deactivated for all default schedules*) states the name assigned to this very schedule by the program vendor. For newly added schedules (*you can add a new schedule by right-clicking over the* ***Scheduled scan*** *item in the left navigation tree*) you can specify your own name, and in that case the text field will open for editing. Try to always use brief, descriptive, and apt names for scans to make it easier to later differentiate the scan from others.

Example: *It is not appropriate to call the scan by the name "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System area scan" etc. It is also not necessary to specify in the scan's name whether it is the scan of the whole computer or just a scan of selected files or folders - your own scans will always be a specific version of the scan of selected files or folders.*

In this dialog you can further define the following parameters of the scan:

Schedule running

Here, you can specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time (***Run every ...***) or by defining an exact date and time (***Run at specific times***), or possibly by defining an event that the scan launch should be associated with (***Run on computer startup***).

Advanced schedule options

- ***Run on computer startup if task has been missed*** – if you schedule the task to run at a specific time, this option will ensure that the scan will be performed subsequently in case the computer is

turned off at the scheduled time.

- ***Run even if computer is in low power mode*** – the task should be performed even if the computer is running on battery power at the scheduled time.



On the ***Settings*** tab you will find a list of scanning parameters that can be optionally switched on/off. By default, most parameters are switched on and the functionality will be applied during scanning. ***Unless you have a valid reason to change these settings we recommend that you keep the predefined configuration***:

- ***Heal / remove virus infection without asking me*** *(on by default):* if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default):* check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** (*off by default*): mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for tracking cookies*** (*off by default*): this parameter specifies that cookies should be detected during scanning; (*HTTP cookies are used for authenticating, tracking, and maintaining specific*

information about users, such as site preferences or the contents of their electronic shopping carts).

- ***Scan inside archives*** (*off by default*): this parameter specifies that the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...
- ***Use heuristics*** (*on by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning.
- ***Scan system environment*** (*on by default*): scanning will also check the system areas of your computer.
- ***Enable thorough scanning*** (*off by default):* in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.
- ***Scan for rootkits*** *(on by default):* Anti-Rootkit scan searches your computer for possible rootkits, i.e. programs and technologies that can cover malware activity in your computer. If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

You should also decide whether you want to scan

- ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated (*after being saved, the commas change into semicolons*) file extensions that should not be scanned.
- ***Selected file types*** - you can specify that you want to scan only files that can get infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.
- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

Adjust how quickly scan completes

Within this section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the *user sensitive* level of automatic resource usage. If you want the scan to run faster, it will take less time but the system resources used will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease the system resources used by extending the scanning duration.

Set additional scan reports

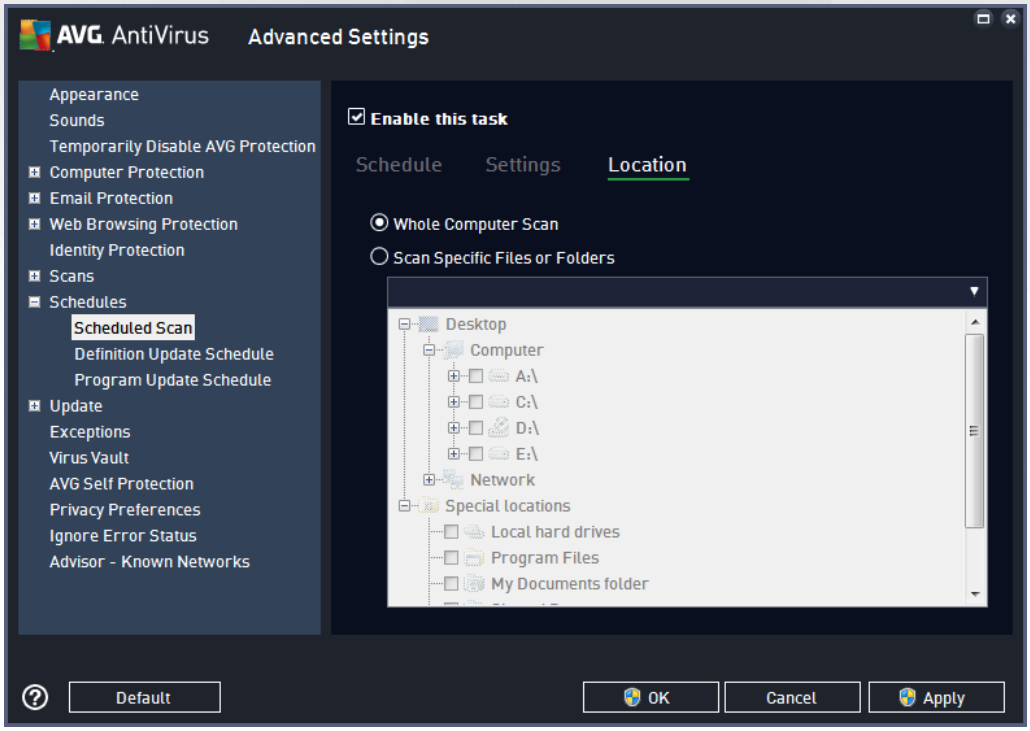
Click the ***Set additional scan reports ...*** link to open a standalone dialog window called ***Scan reports*** where

you can tick several items to define what scan findings should be reported:



Computer shutdown options

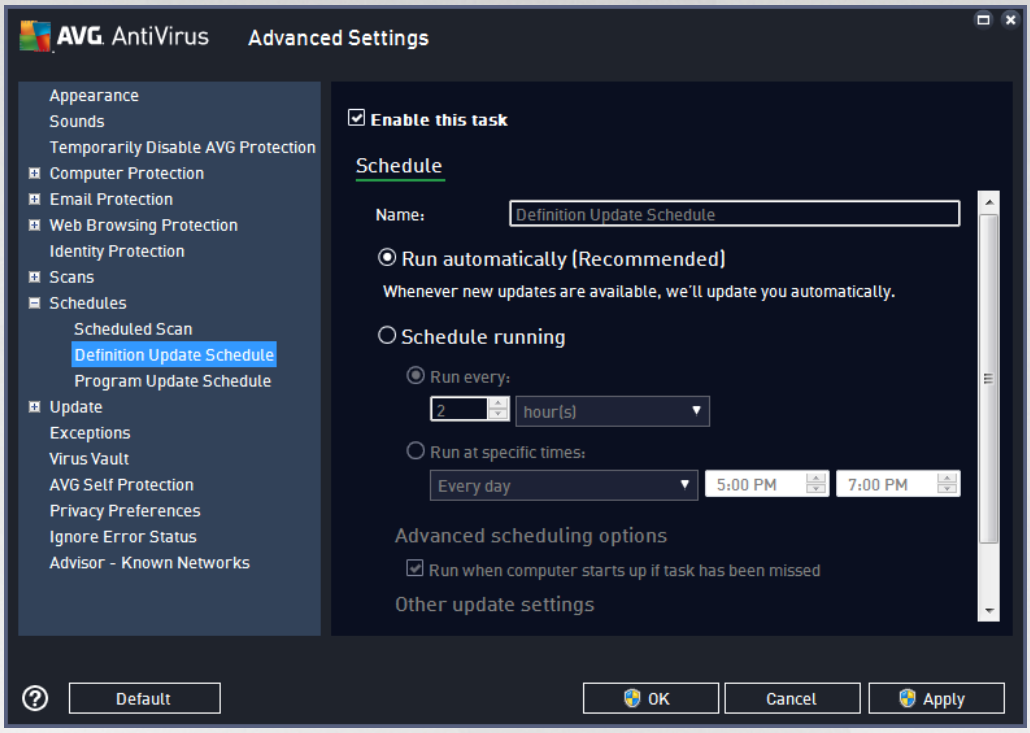
In the ***Computer shutdown options*** section you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown if computer is locked***).



On the ***Location*** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. If you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned.

7.9.2. Definitions Update Schedule

If ***really necessary***, you can uncheck the ***Enable this task*** item to simply deactivate the scheduled definitions update temporarily, and switch it on again later:



Within this dialog you can set up some detailed parameters for the definition update schedule. The text field called ***Name*** (*deactivated for all default schedules*) shows the name assigned to this very schedule by the program vendor.

Schedule running

By default, the task is launched automatically (***Run automatically***) as soon as a new virus definition update is available. We recommend that you stick to this configuration unless you have a good reason to do otherwise! Then, you can set up the task launch manually, and specify the time intervals for the newly scheduled definitions update launch. The timing can either be defined by the repeated update launch after a certain period of time (***Run every ...***) or by defining an exact date and time (***Run at specific times***).

Advanced schedule options

This section allows you to define under which conditions the definition update should/should not be launched if the computer is in low power mode or switched off completely.

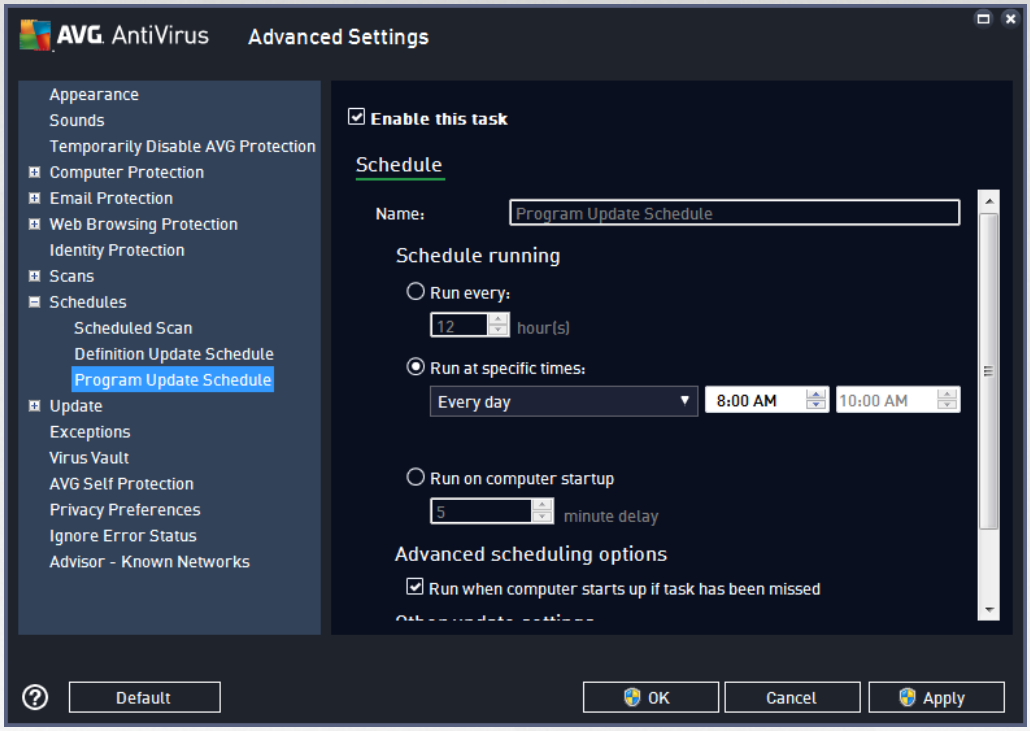
Other update settings

Finally, check the ***Run the update again as soon as the Internet connection is available*** option to make sure than if the Internet connection is interrupted and the update process fails, it will be launched again

immediately after the Internet connection is restored. Once the scheduled update is launched at the time you have specified, you will be informed of this fact via a pop-up window opened over the AVG system tray icon (*provided that you have kept the default configuration of the the Advanced Settings/Appearance dialog*).

7.9.3. Program Update Schedule

If ***really necessary***, you can uncheck the ***Enable this task*** item to simply deactivate the scheduled program update temporarily, and switch it on again later:



The text field called ***Name*** (*deactivated for all default schedules*) shows the name assigned to this very schedule by the program vendor.

Schedule running

Here, specify the time intervals for the newly scheduled program update launch. The timing can either be defined by the repeated update launch after a certain period of time (***Run every***) or by defining an exact date and time (***Run at specific times***), or possibly by defining an event that the update launch should be associated with (***Run on computer startup***).

Advanced schedule options

This section allows you to define under which conditions the program update should/should not be launched if the computer is in low power mode or switched off completely.

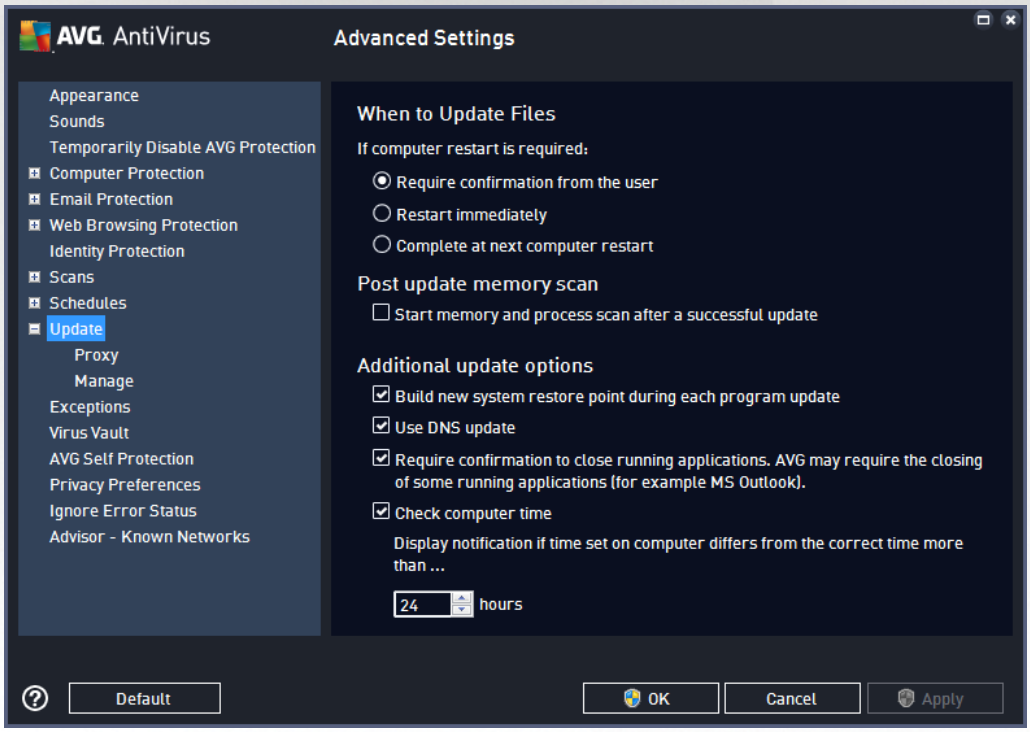
Other update settings

Check the ***Run the update again as soon as the Internet connection is available*** option to make sure that if the Internet connection is interrupted and the update process fails, it will be launched again immediately after the Internet connection is restored. Once the scheduled update is launched at the time you have specified, you will be informed of this fact via a pop-up window opened over the AVG system tray icon (*provided that you have kept the default configuration of the the Advanced Settings/Appearance dialog*).

Note: *If the timings of a scheduled program update and scheduled scan coincide, the update process is of higher priority and the scan will be interrupted. In such a case you will be informed about the collision.*

7.10. Update

The ***Update*** navigation item opens a new dialog where you can specify general parameters regarding the AVG update:



When to update files

In this section you can select three alternative options to be used in case the update process requires your PC to restart. The update finalization can be scheduled for the next PC restart, or you can launch the restart immediately:

- ***Require confirmation from the user*** *(by default)* - you will be asked to approve a PC restart needed to finalize the update process
- ***Restart immediately*** - the computer will be restarted automatically immediately after the update process has finished, and your approval will not be required
- ***Complete at next computer restart*** - the update process finalization will be postponed until the next computer restart. Please keep in mind that this option is only recommended if you are sure to restart

the computer regularly, at least once a day!

Post update memory scan

Mark this checkbox to stipulate that you want to launch a new memory scan after each successfully completed update. The latest downloaded update might have new virus definitions, and these could be applied in the scanning immediately.

Additional update options

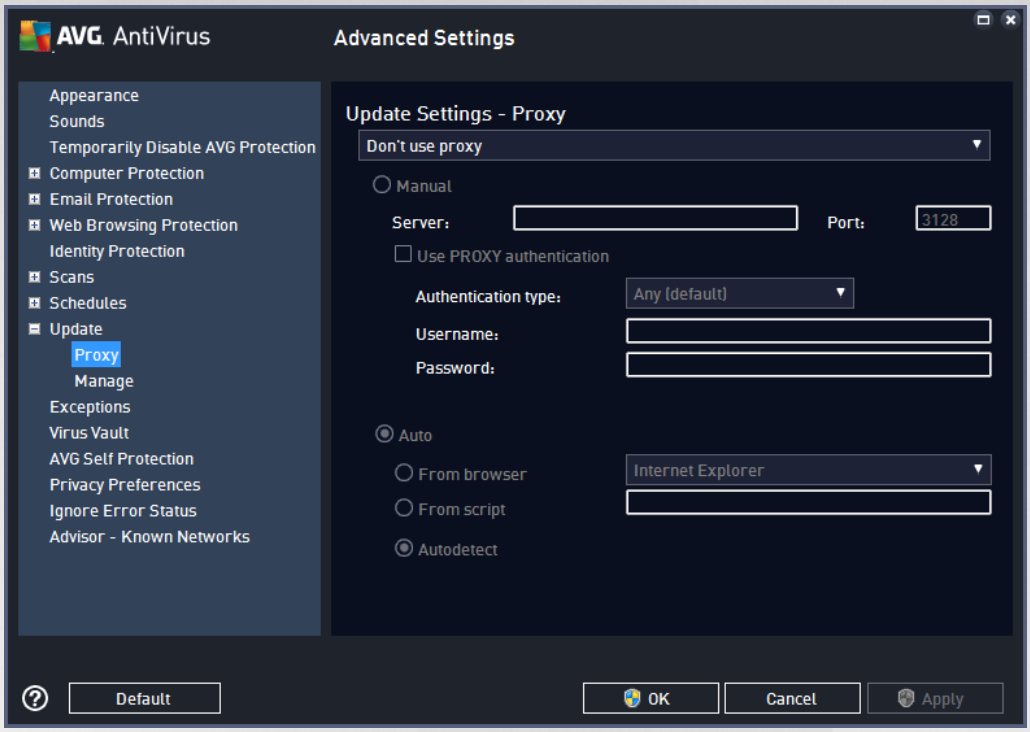
- ***Build new system restore point during each program update*** (*on by default*) - before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS to its original configuration from this point. This option is accessible via Start / All Programs / Accessories / System tools / System Restore, but any changes can be recommended to experienced users only! Keep this check-box ticked if you want to make use of this functionality.

- ***Use DNS update*** (*on by default*) - with this item marked, once the update is launched, your **AVG AntiVirus 2015** looks for information about the latest virus database version and the latest program version on the DNS server. Then only the smallest indispensably required update files are downloaded, and applied. This way the total amount of data downloaded is minimized, and the update process runs faster.

- ***Require confirmation to close running applications*** (*on by default*) - this will help you make sure no currently running applications will be closed without your permission - if required for the update process to be finalized.

- ***Check computer time*** (*on by default*) - mark this option to declare you wish to have notifications displayed in case the computer time differs from the correct time more than by a specified number of hours.

7.10.1. Proxy



The proxy server is a stand-alone server or a service running on a PC that guarantees safer connection to the Internet. According to the specified network rules you can then access the Internet either directly or via the proxy server; both possibilities can also be allowed at the same time. Then, in the first item of the ***Update settings - Proxy*** dialog you have to select from the combo box menu whether you want to:

- ***Don't use proxy*** - default settings
- ***Use proxy***
- ***Try connection using proxy and if it fails, connect directly***

If you select any option using a proxy server, you will have to specify some further data. The server settings can be configured either manually or automatically.

Manual configuration

If you select manual configuration (check *the **Manual** option to activate the respective dialog section*) you have to specify the following items:

- ***Server*** - specify the server's IP address or the name of the server
- ***Port*** - specify the number of the port that enables Internet access (*by default, this number is set to 3128 but can be set differently - if you are not sure, contact your network administrator*)

The proxy server can also have specific rules configured for each user. If your proxy server is set up this way, check the ***Use PROXY authentication*** option to verify that your user name and password are valid for

connecting to the Internet via the proxy server.

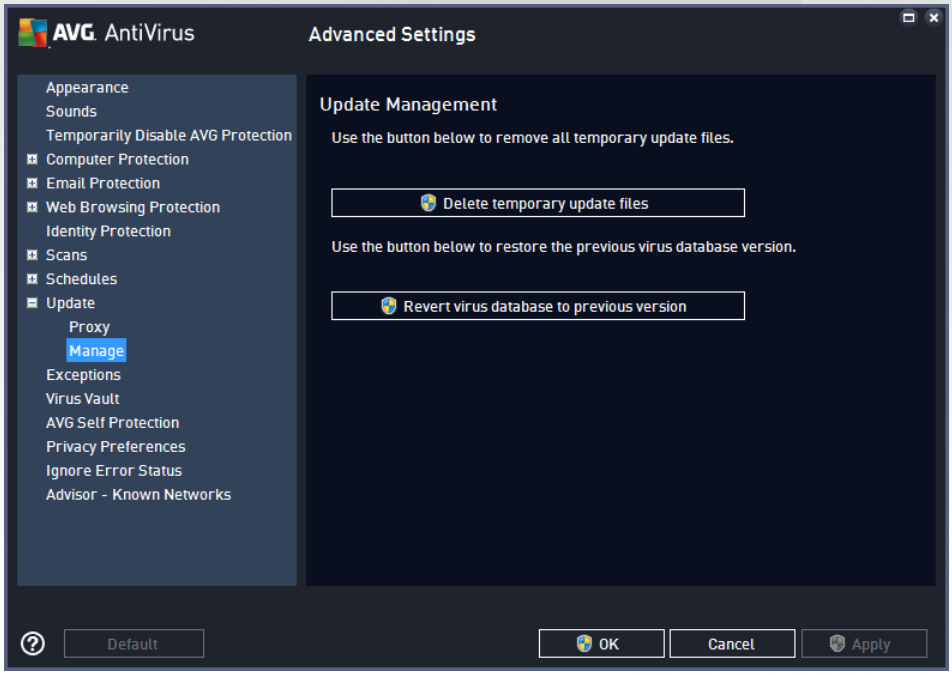
Automatic configuration

If you select automatic configuration (*mark the **Auto** option to activate the respective dialog section*) then please select where the proxy configuration should be taken from:

- ***From browser*** - the configuration will be read from your default Internet browser
- ***From script*** - the configuration will be read from a downloaded script with the function returning the proxy address
- ***Autodetect*** - the configuration will be detected automatically directly from the proxy server

7.10.2. Manage

The ***Update Management*** dialog offers two options accessible via two buttons:



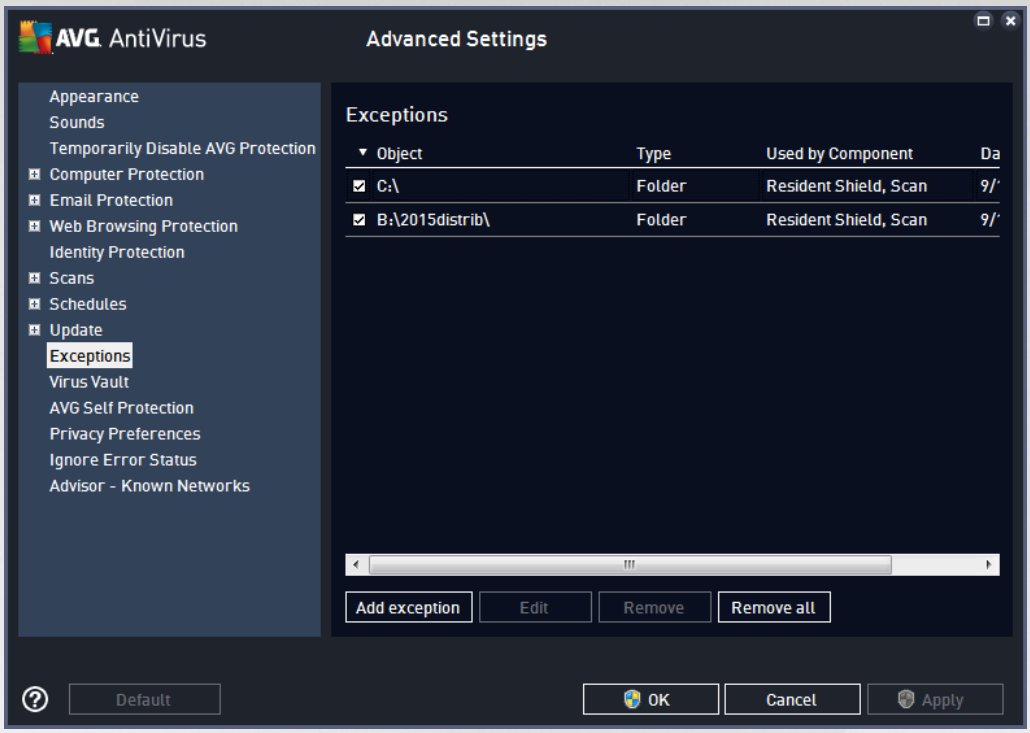
- ***Delete temporary update files*** - press this button to delete all redundant update files from your hard disk (*by default, these files are saved for 30 days*)
- ***Revert virus database to previous version*** - press this button to delete the latest virus base version from your hard disk, and return to the previously saved version (*new virus base version will be a part of the following update*)

7.11. Exceptions

In the ***Exceptions*** dialog you can define exceptions, i.e. items that **AVG AntiVirus 2015** will ignore. Typically, you will need to define an exception if AVG keeps detecting a program or file as a threat, or blocking a safe website as dangerous. Add such file or website to this exception list, and AVG will not report or block it any

more.

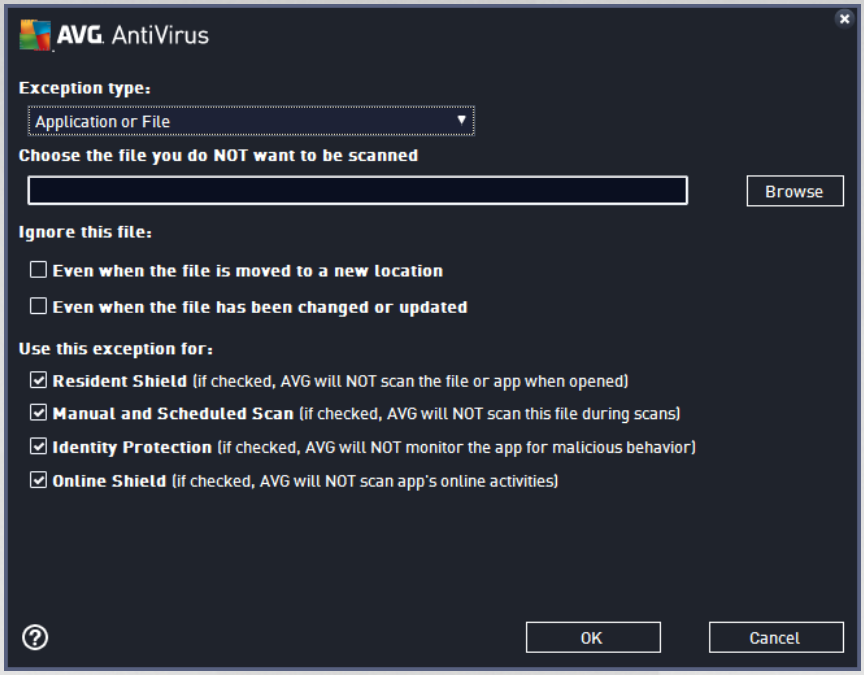
Please always make sure that the file, program or website in question really is absolutely safe!



The chart in the dialog displays a list of exceptions, if any have been already defined. Each item has a checkbox next to it. If the checkbox is marked, then the exception is in effect; if not, then the exception is just defined but not currently used. By clicking a column header, you can sort the allowed items according to the respective criteria.

Control buttons

- ***Add exception*** - Click to open a new dialog where you can specify the item that should be excluded from AVG scanning:



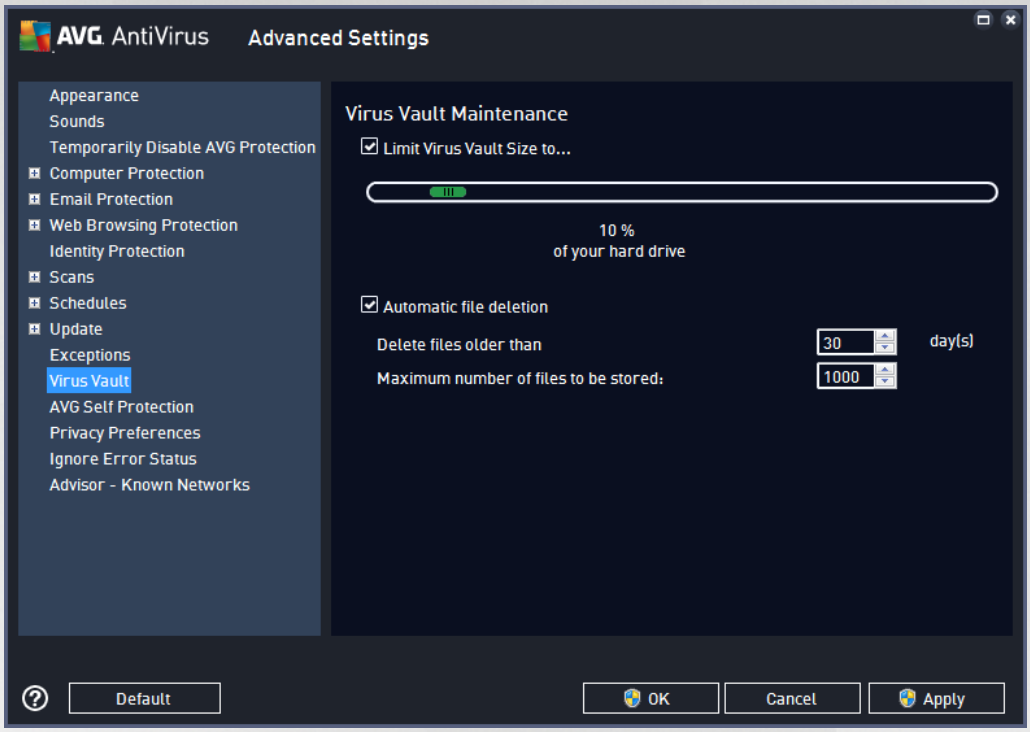
First, you will be invited to define the type of the object, i.e. whether it is an application or a file, a folder, URL, or a certificate. Then you will have to browse your disk to provide the path to the respective object, or type the URL. Finally, you can select what AVG features should ignore the selected object *(Resident Shield, Identity Protection, Scan)*.

- ***Edit*** - This button is only active if some exceptions have been already defined, and are listed in the chart. Then, you can use the button to open the editing dialog over a selected exception, and configure the parameters of the exception.

- ***Remove*** - Use this button to cancel a previously defined exception. You can either remove them one by one, or highlight a block of exceptions in the list and cancel the defined exceptions. Having canceled the exception, the respective file, folder or URL will be checked by AVG again. Please note that only the exception will be removed, not the file or folder itself!

- ***Remove all*** - Use this button to delete all defined exceptions in the list.

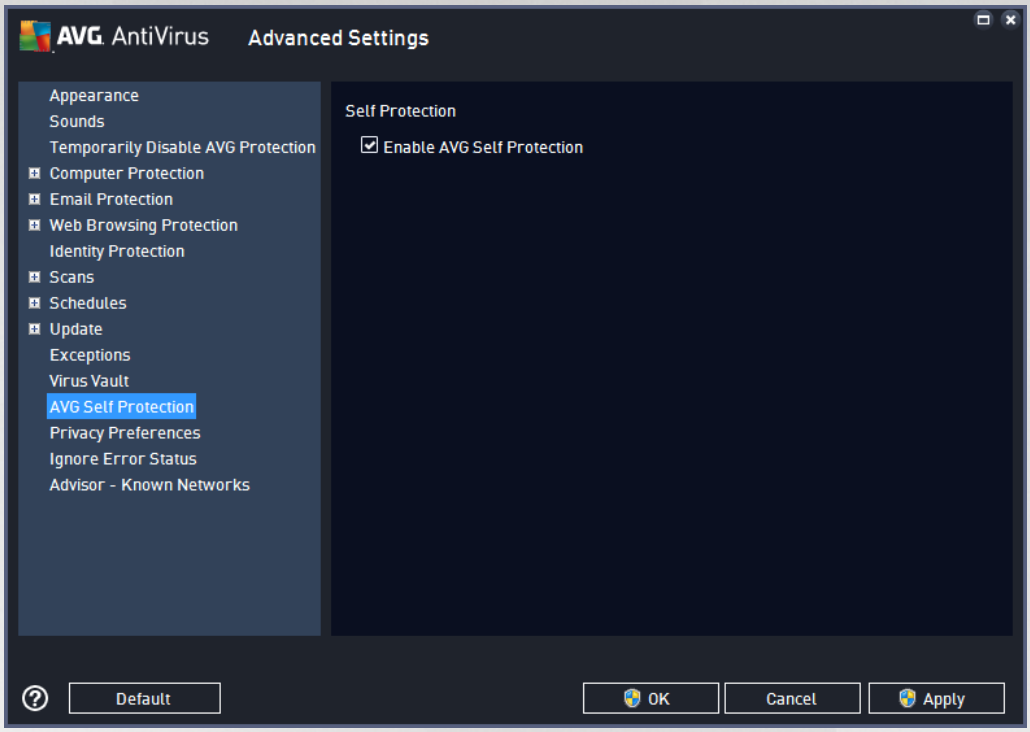
7.12. Virus Vault



The ***Virus Vault Maintenance*** dialog allows you to define several parameters regarding the administration of objects stored in the Virus Vault:

- ***Limit Virus Vault Size*** - use the slider to set up the maximum size of the Virus Vault. The size is specified proportionally compared to the size of your local disk.
- ***Automatic file deletion*** - in this section define the maximum length of time that objects should be stored in the Virus Vault (***Delete files older than ... days***), and the maximum number of files to be stored in the Virus Vault (***Maximum number of files to be stored***).

7.13. AVG Self Protection

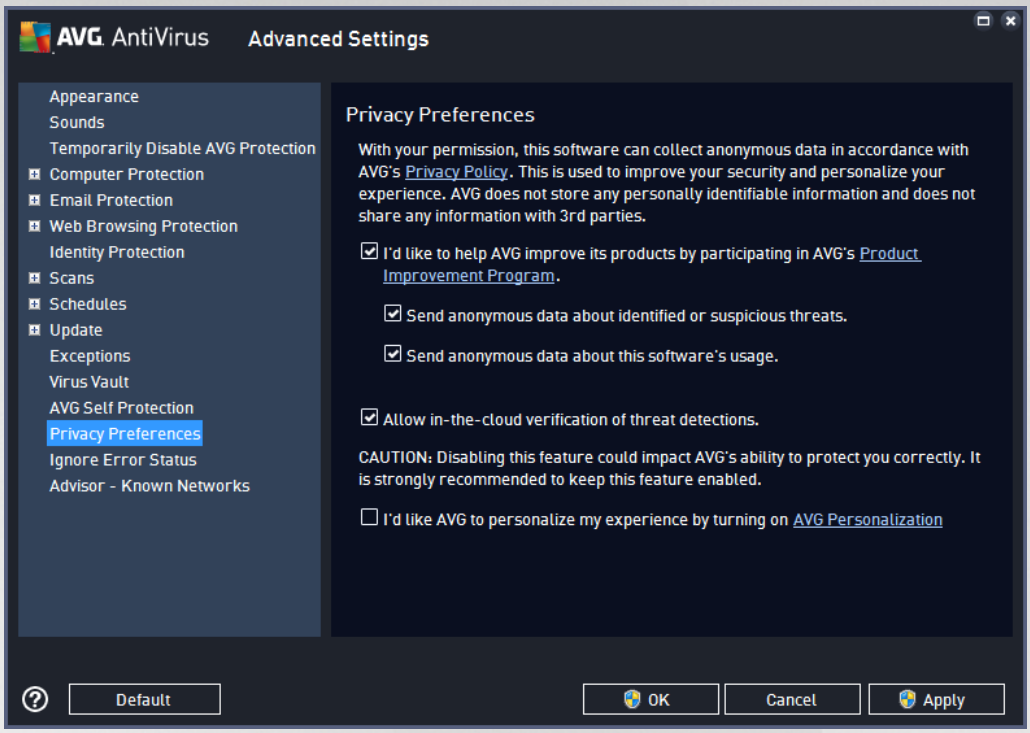


The ***AVG Self Protection*** enables **AVG AntiVirus 2015** to protect its own processes, files, registry keys and drivers from being changed or deactivated. The main reason for this kind of protection is that some sophisticated threats try to disarm the antivirus protection, and then freely cause damage to your computer.

We recommend keeping this feature turned on!

7.14. Privacy Preferences

The ***Privacy Preferences*** dialog invites you to participate in AVG product improvement, and to help us increase the overall Internet security level. Your reporting helps us collect up-to-date information on the latest threats from all participants worldwide, and in return we can improve protection for everyone. The reporting is made automatically, and therefore does not cause you any inconvenience. No personal data is included in the reports. The reporting of detected threats is optional, however, we do ask you to keep this option switched on. It helps us improve protection for both you and other AVG users.

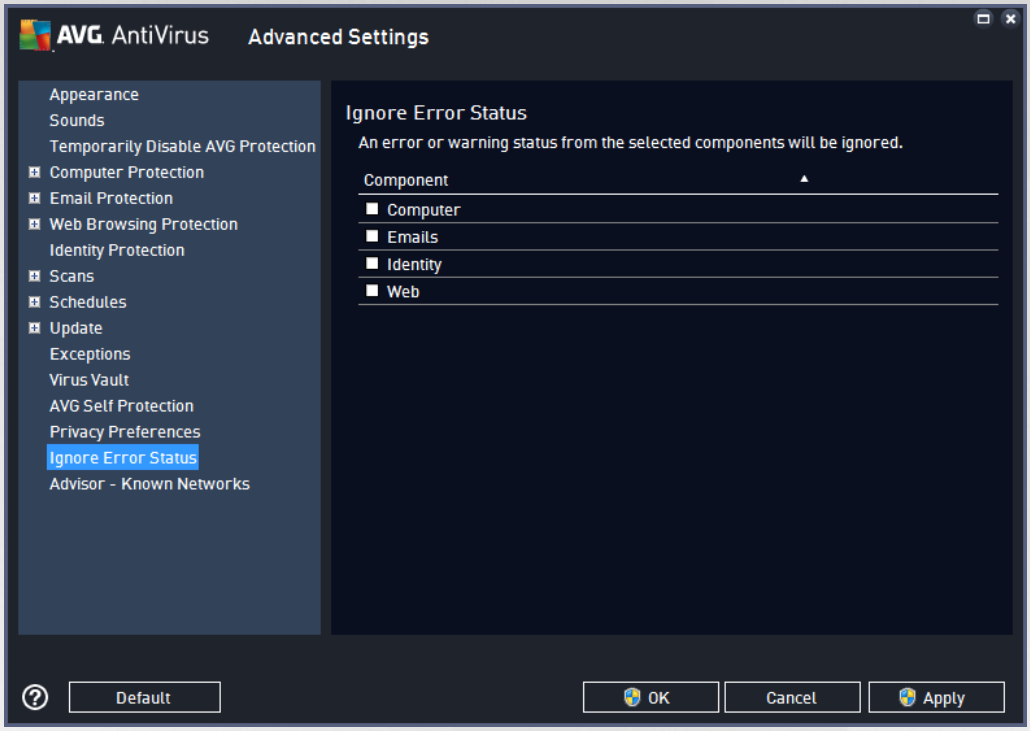


Within the dialog, the following setting options are available:

- ***I'd like to help AVG improve their products by participating in the AVG Product Improvement Program*** *(on by default)* - If you want to help us further improve **AVG AntiVirus 2015**, keep the checkbox marked. This will enable all encountered threats to be reported to AVG, so we will be able to collect up-to-date information on malware from all participants worldwide, and in return improve protection for everyone. The report is made automatically, and therefore does not cause you any inconvenience, and no personal data is included in the reports.
    - ***Allow to send upon user confirmation data about misidentified email*** *(on by default)* - send information about email messages incorrectly identified as spam, or about spam messages that were not detected by the Anti-Spam service. When sending this kind of information, you will be asked for confirmation.
    - ***Allow to send anonymous data about identified or suspicious threats*** *(on by default)* - send information about any suspicious or positively dangerous code or behaviour pattern *(can be a virus, spyware, or malicious webpage your are trying to access)* detected on your computer.
    - ***Allow to send anonymous data about product usage*** *(on by default)* - send basic statistics about the application usage, such as number of detections, scans launched, successful or unsuccessful updates etc.
- ***Allow in the cloud verification of detections*** *(on by default)* - detected threats will be checked if really infected, to sort out false positives.
- ***I'd like AVG to personalize my experience by turning on AVG Personalization*** *(off by default)* - this feature anonymously analyzes behavior of programs and applications installed on your PC. Based on this analysis AVG can offer you services targeted directly to your needs, to secure your maximum safety.

7.15. Ignore Error Status

In the ***Ignore error status*** dialog you can tick those components that you do not want to get informed about:



By default, no component is selected in this list. It means that if any component is given an error status, you will be informed about it immediately via:

- system tray icon - while all parts of AVG are working properly, the icon is displayed in four colors; however, if an error occurs, the icon appears with a yellow exclamation mark,
- text description of the existing problem in the Security Status Info section of the AVG main window

There might be a situation that for some reason you need to switch a component off temporarily. ***This is not recommended, you should try to keep all components permanently on and in default configuration***, but it may happen. In this case the system tray icon automatically reports the component's error status. However, in this very case we cannot talk about an actual error since you have deliberately induced it yourself, and you are aware of the potential risk. At the same time, once being displayed in grey color, the icon cannot actually report any possible further error that might appear.

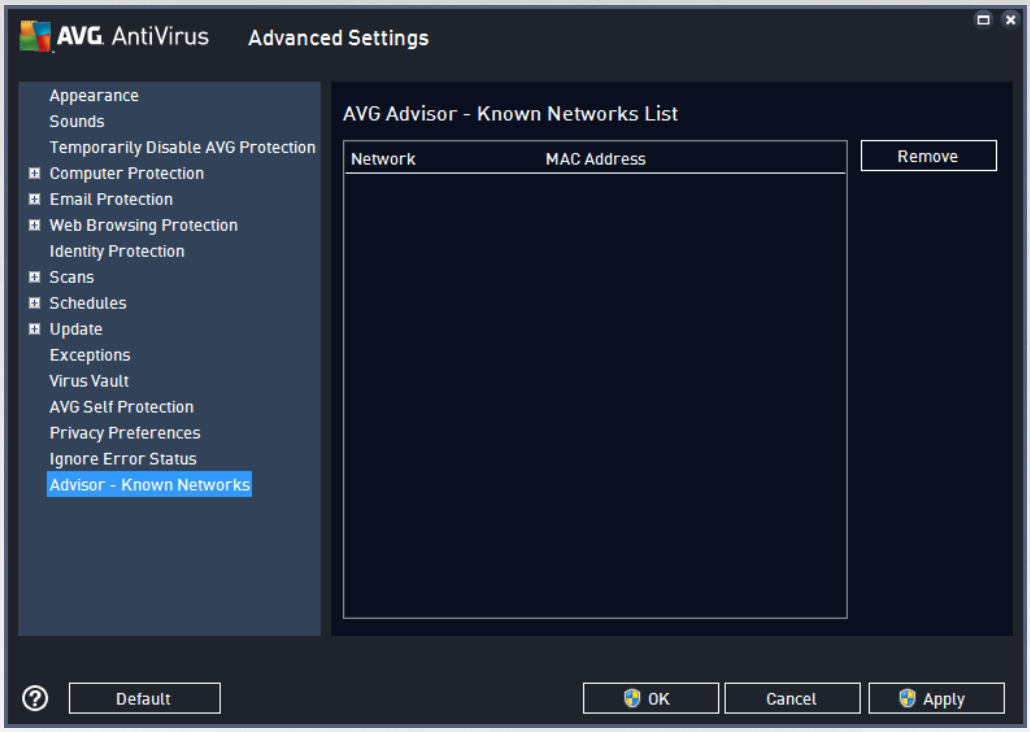
For this situation, within the ***Ignore error status*** dialog you can select components that may be in an error state (*or switched off*) and you do not wish to receive information about it. Press the ***OK*** button to confirm.

7.16. Advisor - Known Networks

The AVG Advisor includes a feature that monitors networks you connect to, and if a new network is found *(with an already used network name, which can lead to confusion)* it will notify you and recommend that you check the network's safety. If you decide that the new network is safe to connect to, you can also save it to this list *(Via the link provided in the AVG Advisor tray notification that slides over the system tray once an unknown network is detected. For details please see chapter on AVG Advisor)*. AVG Advisor will then remember the

unique attributes of the network *(specifically the MAC address)*, and will not display the notification next time. Each network that you connect to will be automatically considered the known network, and added to the list. You can delete individual entries by pressing the ***Remove*** button; the respective network will then be considered unknown and potentially unsafe again.

In this dialog window, you can check which networks are considered to be known:



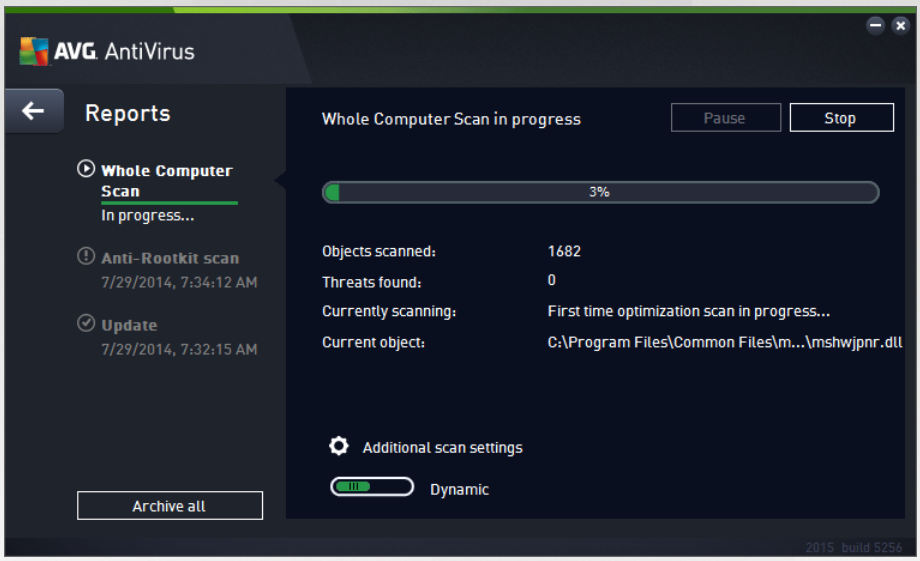
Note: *The known networks feature within AVG Advisor is not supported at Windows XP 64-bit.*

8. AVG Scanning

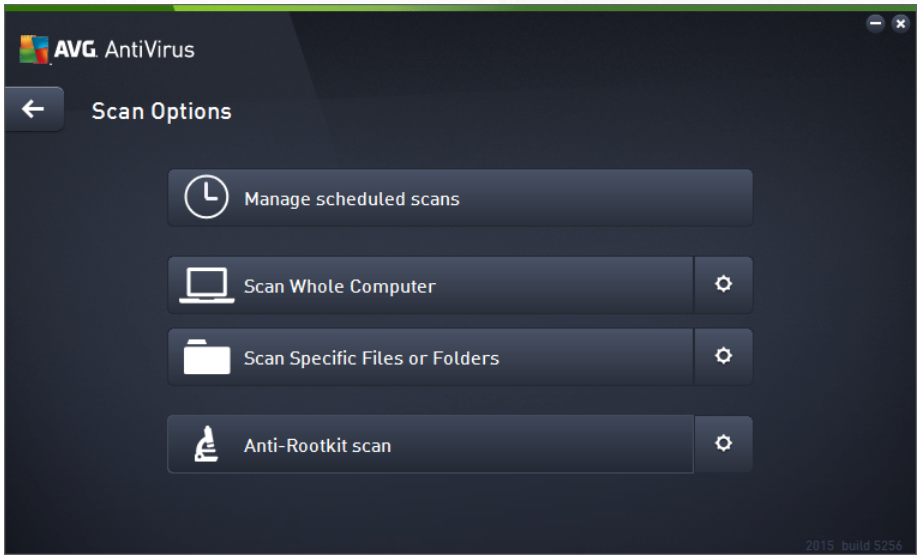
By default, **AVG AntiVirus 2015** does not run any scans, as after the initial one *(that you will be invited to launch*), you should be perfectly protected by the resident components of **AVG AntiVirus 2015** that are always on guard, and do no let any malicious code get into your computer. Of course, you can schedule a scan to run at regular intervals, or manually launch a scan according to your needs any time.

The AVG scanning interface is accessible from the main user interface via the button graphically divided into two sections: 

- ***Scan now*** - Press the button to link to launch the Whole Computer Scan immediately, and watch its progress and results in the automatically opened Reports window:



- ***Options*** - Select this button *(graphically displayed as three horizontal lines in a green field)* to open the ***Scan Options*** dialog where you can manage scheduled scans and edit parameters of the Whole Computer Scan / Scan of Specific Files or Folders.



In the ***Scan Options*** dialog, you can see three main scan configuration sections:

- ***Manage schedules scans*** - Click this option to open a new dialog with an overview of all scan schedules. Before you define your own scans, you will only be able to see one scheduled scan predefined by the software vendor listed in the chart. The scan is turned off, by default. To turn it on, right-click on it and select the *Enable task* option from the context menu. Once the scheduled scan is enabled, you may edit its configuration via the *Edit scan schedule* button. You can also click the *Add scan schedule* button to create a new scan schedule of your own.

- ***Scan whole computer / Settings*** - The button is divided into two sections. Click the *Scan whole computer* option to immediately launch the scanning of the entire of your computer *(for details on the scan of the whole computer please see the respective chapter called Predefined scans / Scan whole computer)*. Clicking the *Settings* section will take you to the configuration dialog of the whole computer scan.

- ***Scan specific files or folders / Settings*** - Again, the button is divided into two sections. Click the *Scan specific files or folders* option to immediately launch the scanning of selected areas of your computer *(for details on the scan of the selected files or folders please see the respective chapter called Predefined scans / Scan specific files or folders)*. Clicking the *Settings* section will take you to the configuration dialog of the specific files or folders scan.

- ***Scan computer for rootkits / Settings*** - The left section of the button labeled *Scan computer for rootkits* launches the immediate anti-rootkit scanning *(for details on the rootkit scan please see the respective chapter called Predefined scans / Scan computer for rootkits).* Clicking the *Settings* section will take you to the configuration dialog of the rootkit scan .

8.1. Predefined Scans

One of the main features of **AVG AntiVirus 2015** is on-demand scanning. On-demand tests are designed to scan various parts of your computer whenever suspicion about possible virus infection arises. Anyway, it is strongly recommended that you carry out such tests regularly even if you think that no virus can be found on your computer.

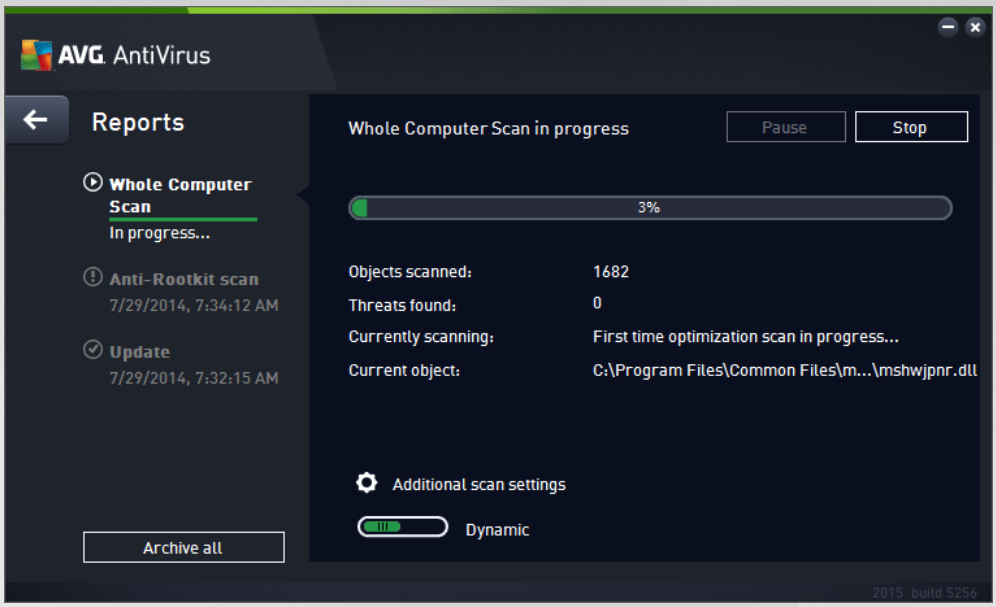
In the **AVG AntiVirus 2015** you will find the following types of scan predefined by the software vendor:

8.1.1. Scan whole computer

Whole computer scan scans your entire computer for possible infections and/or potentially unwanted applications. This test will scan all hard drives on your computer, will detect and heal any virus found, or remove the detected infection to the Virus Vault. Scanning the whole of your computer should be scheduled on your computer at least once a week.

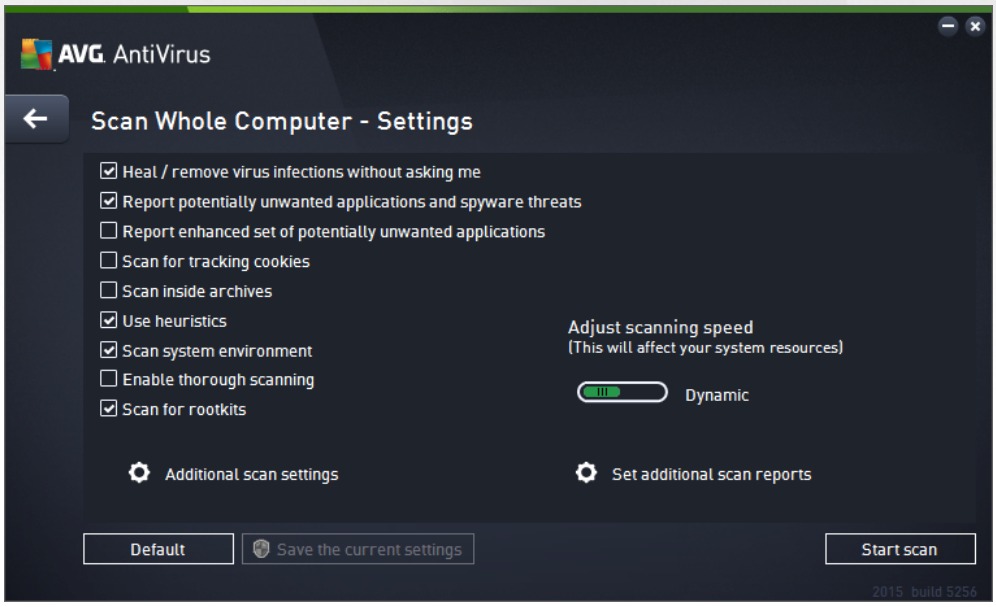
Scan launch

The ***Whole computer scan*** can be launched directly from the main user interface by clicking on the ***Scan now*** button. No further specific settings have to be configured for this type of scan; the scan will start immediately. Within the ***Whole computer scan in progress*** dialog (*see screenshot*) you can watch its progress and results. The scan can be temporarily interrupted (***Pause***) or canceled (***Stop***) if needed.



Scan configuration editing

You can edit the ***Whole computer scan*** configuration in the ***Scan whole computer - Settings*** dialog *(the dialog is accessible via the Settings link for the Whole computer scan within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***



In the list of scanning parameters you can switch on/off specific parameters as needed:

- ***Heal / remove virus infection without asking me*** *(on by default)* - If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default)* - Check to activate the scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** *(off by default)* - Mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for Tracking Cookies*** *(off by default)* - This parameter specifies that cookies should be detected *(HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts)*.

- ***Scan inside archives*** *(off by default)* - This parameter specifies that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

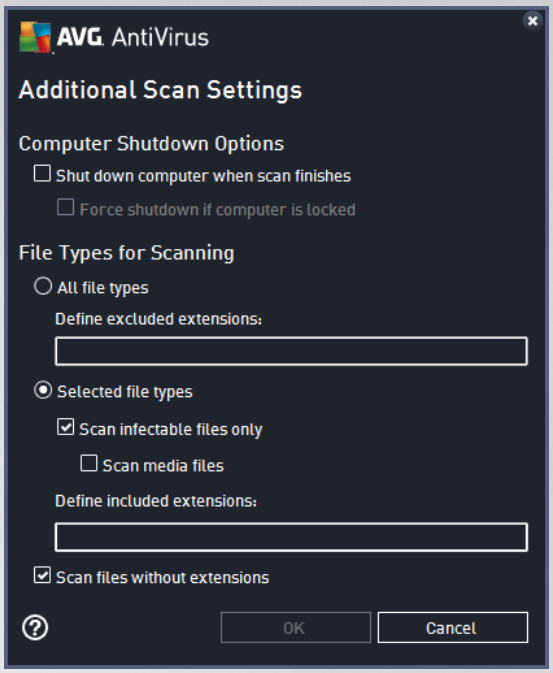
- ***Use Heuristics*** *(on by default)* - Heuristic analysis *(dynamic emulation of the scanned object's instructions in a virtual computer environment)* will be one of the methods used for virus detection during scanning.

- ***Scan system environment*** *(on by default)* - Scanning will also check the system areas of your computer.

- ***Enable thorough scanning*** *(off by default)* - In specific situations *(suspicions about your computer being infected)* you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

- ***Scan for rootkits*** *(on by default)*: includes anti-rootkit scanning into the scanning of the whole computer. The anti-rootkit scan can be also launched separately.

- ***Additional scan settings*** - the link opens a new Additional scan settings dialog where you can specify the following parameters:



- ***Computer shutdown options*** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown if computer is locked***).

- ***File types for scanning*** - you should also decide whether you want scan:

  - ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned;

  - ***Selected file types*** - you can specify that you want to scan only files that can be infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.

  - Optionally, you can decide to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

- ***Adjust how quickly scan completes*** - you can use the slider to change the scanning process priority. By default, this option value is set to the *user sensitive* level of automatic resource usage. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resource requirements (*e.g. when the computer is temporarily unattended*).

- ***Set additional scan reports*** - the link opens a new ***Scan reports*** dialog where you can select what types of possible findings should be reported:



Warning: *These scan settings are identical to the parameters for a newly defined scan - as described in the AVG Scanning / Scan scheduling/ How to Scan chapter. Should you decide to change the default configuration of the* ***Scan the whole computer*** *you can then save your new setting as the default configuration to be used for all further scans for the whole computer.*

8.1.2. Scan specific files or folders

Scan Specific Files or Folders - scans only those areas of your computer that you have selected to be scanned (*selected folders, hard disks, floppy discs, CDs, etc.*). The scanning progress in case of virus detection and its treatment is the same as when scanning the whole computer: any virus found is healed or removed to the Virus Vault. Specific files or folders scanning can be used to set up your own tests and their scheduling based on your needs.

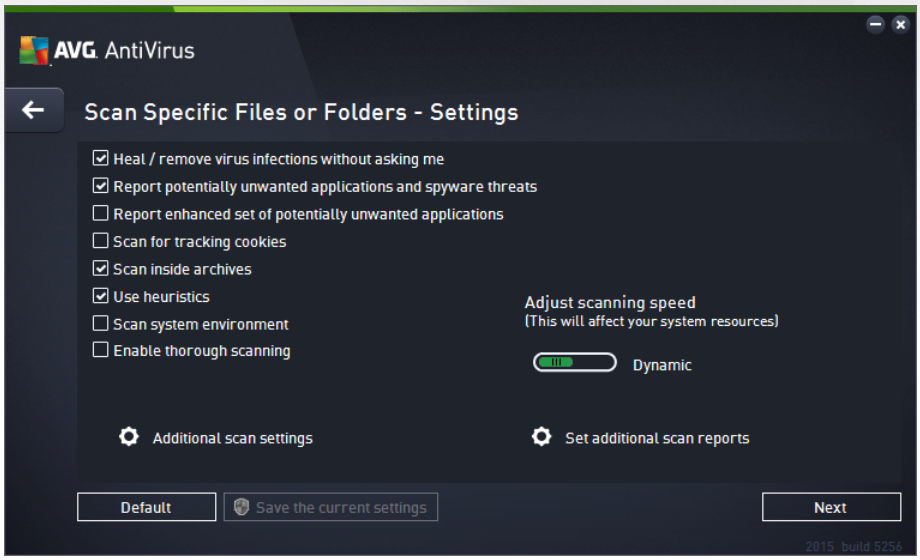
Scan launch

The ***Scan of specific files or folders*** can be launched directly from the Scan options dialog by clicking on the **Scan specific files or folders** button. A new dialog called ***Select specific files or folders for scanning*** opens. In the tree structure of your computer select those folders you want to scan. The path to each selected folder will be generated automatically and appear in the text box in the upper part of this dialog. There is also the option of having a specific folder scanned while all its sub folders are excluded from this scan; to do that write a minus sign "**-**" in front of the automatically generated path (*see screenshot*). To exclude the entire folder from scanning use the "!" parameter. Finally, to launch the scan, press the ***Start scan*** button; the scanning process itself is basically identical to the Whole computer scan.



Scan configuration editing

You can edit the ***Scan Specific Files or Folders*** configuration in the ***Scan Specific Files or Folders - Settings*** dialog *(the dialog is accessible via the Settings link for the Scan specific files or folders within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***



In the list of scanning parameters you can switch specific parameters on/off as needed:

- ***Heal / remove virus infection without asking me*** *(on by default)*: If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default)*: Check to activate

scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** *(off by default)*: Mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for Tracking Cookies*** *(off by default)*: This parameter specifies that cookies should be detected *(HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts)*.

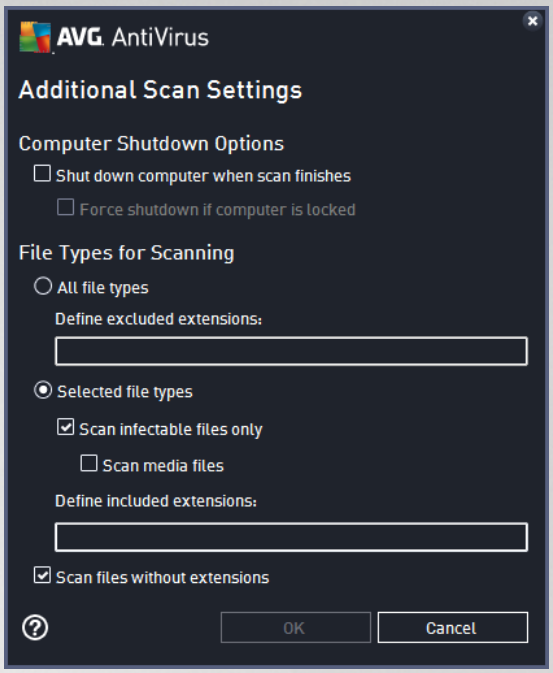
- ***Scan inside archives*** *(on by default)*: This parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

- ***Use Heuristics*** *(on by default)*: Heuristic analysis *(dynamic emulation of the scanned object's instructions in a virtual computer environment)* will be one of the methods used for virus detection during scanning.

- ***Scan system environment*** *(off by default)*: Scanning will also check the system areas of your computer.

- ***Enable thorough scanning*** *(off by default)*: In specific situations *(suspicions about your computer being infected)* you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

- ***Additional scan settings*** - The link opens a new ***Additional scan settings*** dialog where you can specify the following parameters:



- ***Computer shutdown options*** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown if computer is locked***).

- ***File types for scanning*** - you should also decide whether you want to scan:

  - ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned;

  - ***Selected file types*** - you can specify that you want to scan only files that can be infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.

  - Optionally, you can decide to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

- ***Adjust how quickly scan completes*** - you can use the slider to change the scanning process priority. By default, this option value is set to the *user sensitive* level of automatic resource usage. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).

- ***Set additional scan reports*** - the link opens a new ***Scan Reports*** dialog where you can select what types of potential findings should be reported:



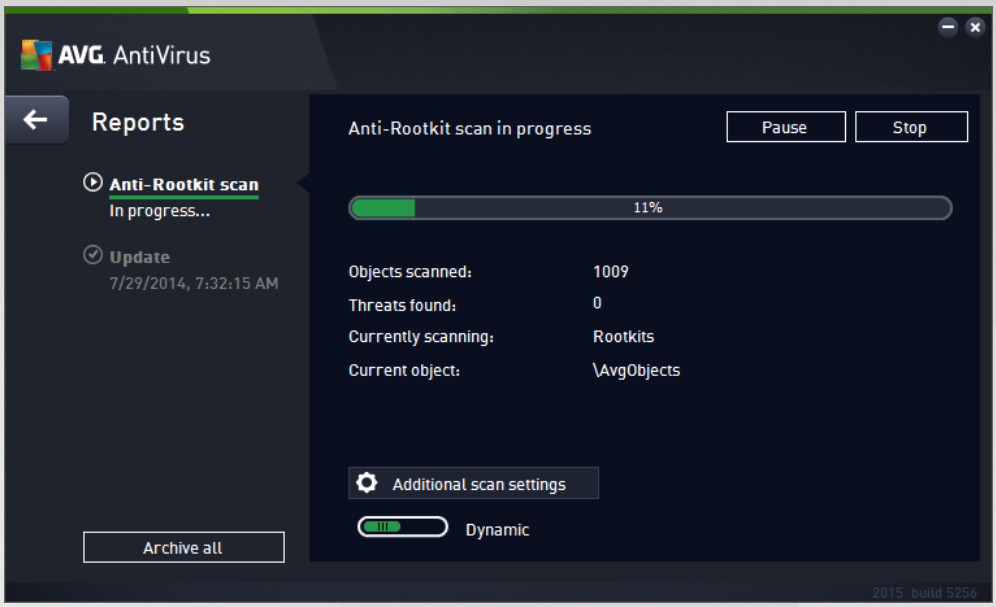
Warning: *These scan settings are identical to the parameters for a newly defined scan - as described in the AVG Scanning / Scan scheduling/ How to Scan chapter. Should you decide to change the default configuration of the* ***Scan specific files or folders*** *you can then save your new setting as the default configuration to be used for all further scans of specific files or folders. Also, this configuration will be used as a template for all of your newly scheduled scans (all customized scans are based on the current configuration of the Scan of selected files or folders).*

8.1.3. Scan computer for rootkits

Scan computer for rootkits is detecting and effectively removing dangerous rootkits, i.e. programs and technologies that can camouflage the presence of malicious software on your computer. A rootkit is designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. The scan is able to detect rootkits based on a predefined set of rules. If a rootkit is found, it does not necessarily mean it is infected. Sometimes, rootkits are used as drivers or they are a part of correct applications.

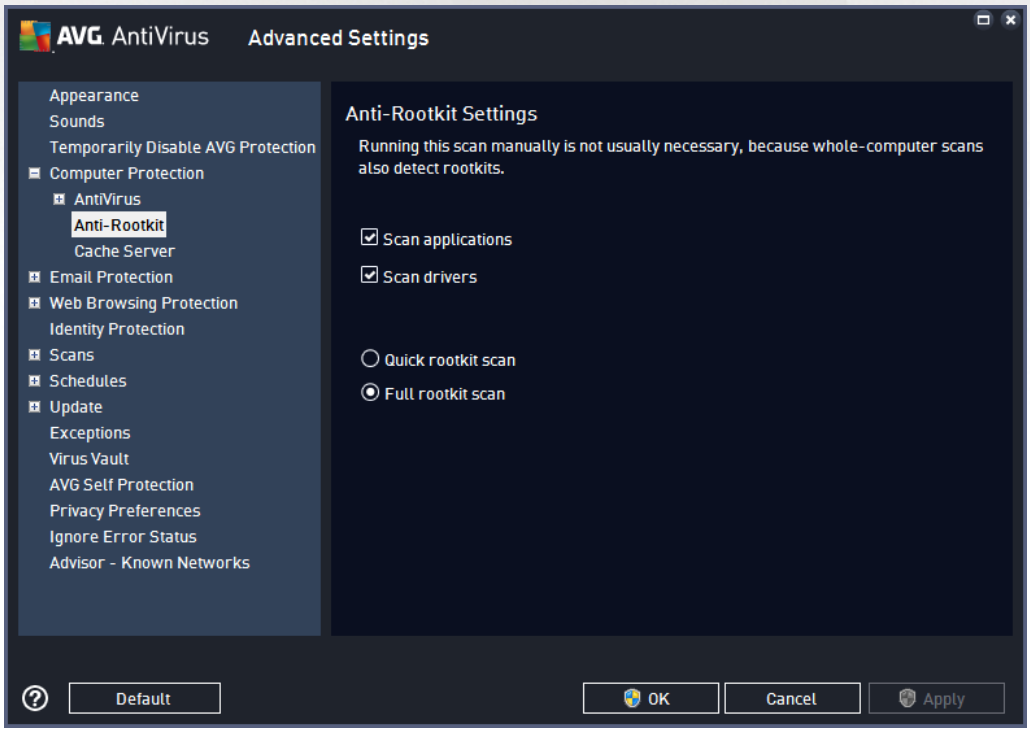
Scan launch

Scan computer for rootkits can be launched directly from the Scan options dialog by clicking on the ***Scan computer for rootkits*** button. A new dialog called ***Anti-rootkit scan in progress*** opens showing the progress of the launched scan:



Scan configuration editing

You can edit the Anti-Rootkit scan configuration in the ***Anti-Rootkit Settings*** dialog *(the dialog is accessible via the Settings link for the Scan computer for rootkits scan within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***

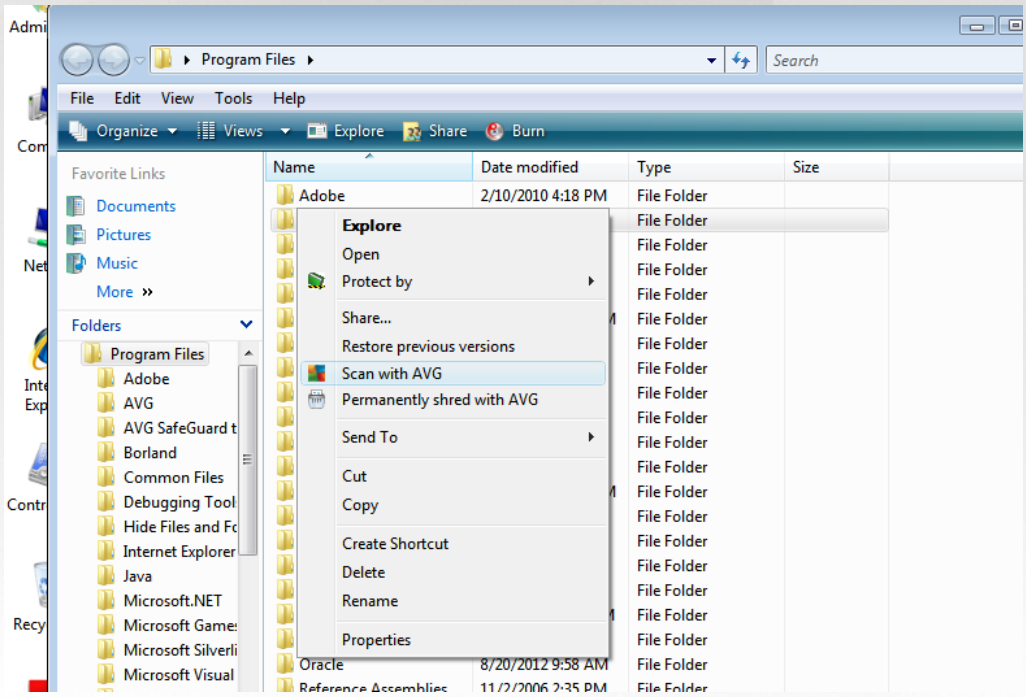


Scan applications and ***Scan drivers*** enable you to specify in detail what should be included in anti-rootkit scanning. These settings are intended for advanced users; we recommend that you keep all options switched on. You can also pick the rootkit scanning mode:

- ***Quick rootkit scan*** - scans all running processes, all loaded drivers, and also the system folder (*most typically c:\Windows*)
- ***Full rootkit scan*** - scans all running processes, all loaded drivers, and also the system folder (*most typically c:\Windows*), plus all local disks (*including the flash disk, but excluding floppy disk/CD drives*)

8.2. Scanning in Windows Explorer

Besides the pre-defined scans launched for the entire computer or its selected areas, **AVG AntiVirus 2015** also offers the option of quick scanning of a specific object directly in the Windows Explorer environment. If you want to open an unknown file and you cannot be sure of its content, you may want to have it checked on demand. Follow these steps:



- Within Windows Explorer highlight the file *(or folder)* you want to check
- Right-click your mouse over the object to open the context menu
- Select the ***Scan with AVG*** option to have the file scanned with **AVG AntiVirus 2015**

8.3. Command Line Scanning

Within **AVG AntiVirus 2015** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scan with most parameters as offered in the AVG graphical user interface.

To launch the AVG scan from the command line, run the following command within the folder where AVG is installed:

- ***avgscanx*** for 32 bits OS
- ***avgscana*** for 64 bits OS

Syntax of the command

The syntax of the command follows:

- ***avgscanx /parameter*** ... e.g. ***avgscanx /comp*** for scanning the whole computer
- ***avgscanx /parameter /parameter*** .. with multiple parameters these should be lined up in a row and separated by a space and a slash character
- if a parameter requires specific value to be provided (e.g. the ***/scan*** parameter that requires information on the selected areas of your computer that are to be scanned, and you have to provide an exact path to the selected section), the values are separated by semicolons, for instance: ***avgscanx /scan=C:\;D:***

Scanning parameters

To display a complete overview of available parameters, type the respective command together with the parameter /? or /HELP (e.g. ***avgscanx /?***). The only obligatory parameter is /SCAN to specify what areas of the computer should be scanned. For a more detailed explanation of the options, see the command line parameters overview.

To run the scan press ***Enter***. During scanning you can stop the process using ***Ctrl+C*** or ***Ctrl+Pause***.

CMD scanning launched from graphic interface

When you run your computer in Windows Safe Mode, there is also an option to launch the command line scan from the graphic user interface. The scan itself will be launched from the command line, the ***Command Line Composer*** dialog only allows you to specify most scanning parameters in the comfortable graphic interface.

Since this dialog is only accessible within the Windows Safe Mode, for a detailed description of this dialog please consult the help file opened directly from the dialog.

8.3.1. CMD Scan Parameters

There follows a list of all parameters available for command line scanning:

- /SCAN Scan specific files or folders /SCAN=path;path *(e.g. /SCAN=C:\;D:\)*
- /COMP Whole Computer scan
- /HEUR Use heuristic analysis
- /EXCLUDE Exclude path or files from scan
- /@ Command file /file name/

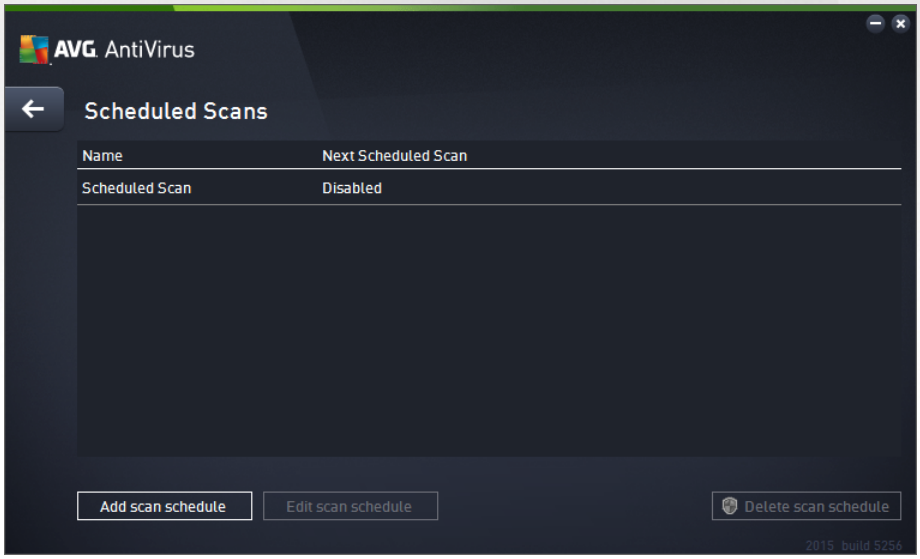
- /EXT Scan these extensions /for example EXT=EXE,DLL/
- /NOEXT Do not scan these extensions /for example NOEXT=JPG/
- /ARC Scan archives
- /CLEAN Clean automatically
- /TRASH Move infected files to the Virus Vault
- /QT Quick test
- /LOG Generate a scan result file
- /MACROW Report macros
- /PWDW Report password-protected files
- /ARCBOMBSW Report archive bombs *(repeatedly compressed archives)*
- /IGNLOCKED Ignore locked files
- /REPORT Report to file /file name/
- /REPAPPEND Append to the report file
- /REPOK Report uninfected files as OK
- /NOBREAK Do not allow CTRL-BREAK to abort
- /BOOT Enable MBR/BOOT check
- /PROC Scan active processes
- /PUP Report Potentially unwanted applications
- /PUPEXT Report enhanced set of Potentially unwanted applications
- /REG Scan registry
- /COO Scan cookies
- /? Display help on this topic
- /HELP Display help on this topic
- /PRIORITY Set scan priority /Low, Auto, High/ *(see Advanced settings / Scans)*
- /SHUTDOWN Shutdown computer upon scan completion
- /FORCESHUTDOWN Force computer shutdown upon scan completion
- /ADS Scan Alternate Data Streams *(NTFS only)*

- /HIDDEN Report files with hidden extensions
- /INFECTABLEONLY Scan files with infectable extensions only
- /THOROUGHSCAN Enable thorough scanning
- /CLOUDCHECK Check for false positives
- /ARCBOMBSW Report re-compressed archive files

8.4. Scan Scheduling

With **AVG AntiVirus 2015** you can run scan on demand *(for instance when you suspect an infection has penetrated your computer)* or based on a scheduled plan. It is highly recommended that you run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan. You should launch the Whole Computer scan regularly, at least once a week. However, if possible, launch the scan of your entire computer daily - as set up in the scan schedule default configuration. If the computer is "always on" then you can schedule scans out of working hours. If the computer is sometimes switched off, then schedule scans to occur on computer start-up when the task has been missed.

The scan schedule can be created / edited in the ***Scheduled scans*** dialog that is accessible via the ***Manage scheduled scan*** button within the Scan options dialog. In the new ***Scheduled Scan*** dialog you can see a complete overview of all currently scheduled scans:

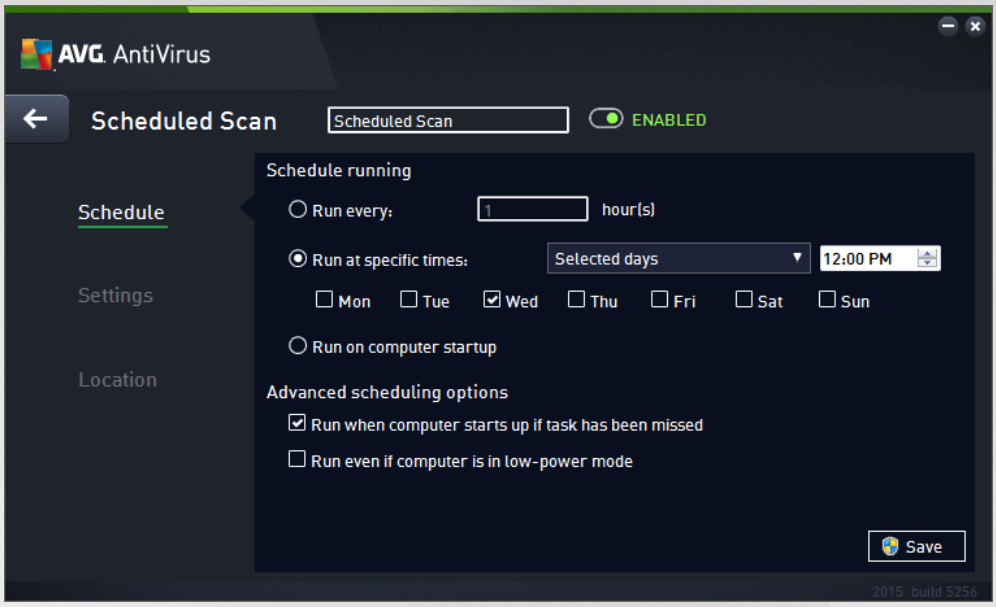


In the dialog you can specify your own scans. Use the ***Add scan schedule*** button to create a new scan schedule of your own. The parameters of the scheduled scan can be edited (*or a new schedule set up*) on three tabs:

- Schedule
- Settings
- Location

On each tab you can simply switch the "traffic light" button to deactivate the scheduled test temporarily, and switch it on again as the need arises.

8.4.1. Schedule



In the upper part of the ***Schedule*** tab you can find the text field where you can specify the name of the scan schedule that is currently being defined. Try to always use brief, descriptive, and apt names for scans to make it easier to later differentiate the scan from others. For example, it is not appropriate to call the scan by the name "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System area scan" etc.

In this dialog you can further define the following parameters of the scan:

- ***Schedule running*** - Here, you can specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time *(Run every ...)* or by defining an exact date and time *(Run at specific times)*, or possibly by defining an event that the scan launch should be associated with *(Run on computer startup)*.

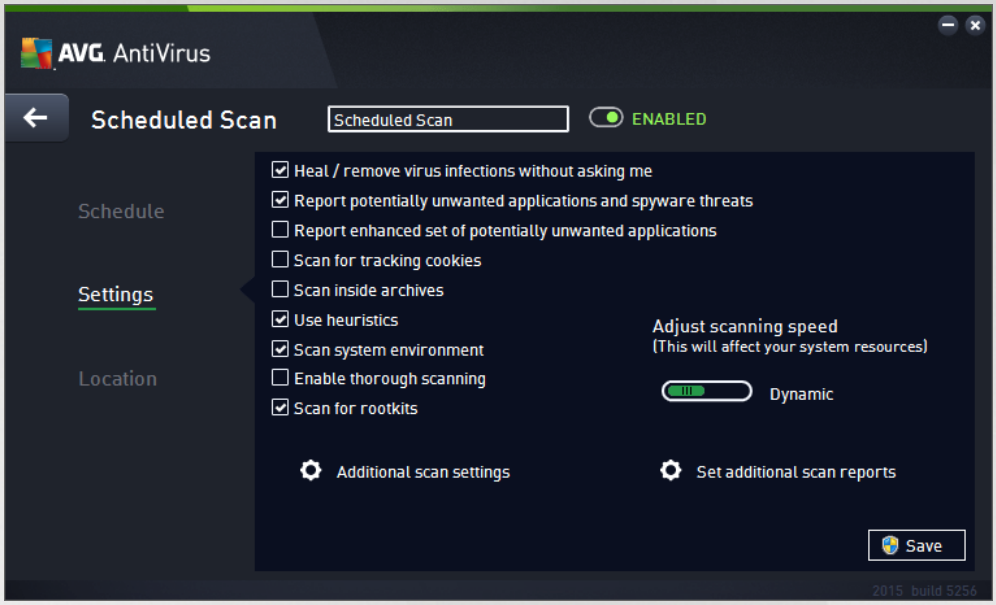
- ***Advanced schedule options*** - This section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely. Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the AVG system tray icon. A new AVG system tray icon then appears (in full color with a flash light) informing a scheduled scan is running. Right-click on the running scan AVG icon to open a context menu where you can decide to pause or even stop the running scan, and also change the priority of the currently running scan.

Controls in the dialog

- ***Save*** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.

- ← - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

8.4.2. Settings



In the upper part of the ***Settings*** tab you can find the text field where you can specify the name of the scan schedule that is currently being defined. Try to always use brief, descriptive, and apt names for scans to make it easier to later differentiate the scan from others. For example, it is not appropriate to call the scan by the name "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System area scan" etc.

On the ***Settings*** tab you will find a list of scanning parameters that can be optionally switched on/off. ***Unless you have a valid reason to change these settings we recommend that you keep the predefined configuration***:

- ***Heal / remove virus infection without asking me*** *(on by default):* if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default):* check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

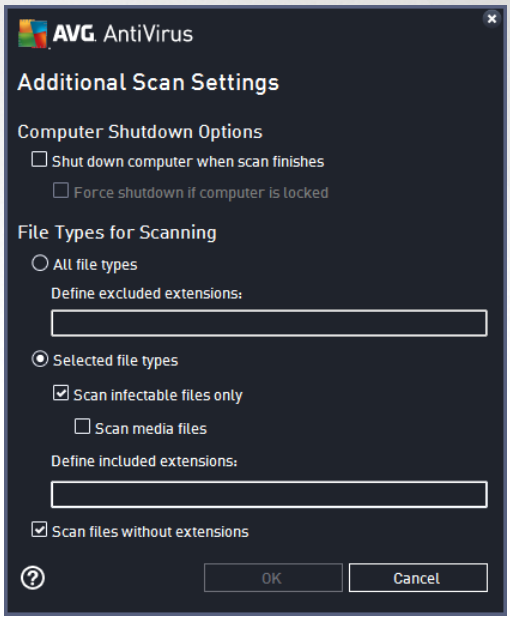
- ***Report enhanced set of potentially unwanted applications*** (*off by default*): mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for tracking cookies*** (*off by default*): this parameter specifies that cookies should be detected during scanning; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*).

- ***Scan inside archives*** (*off by default*): this parameter specifies that the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...
- ***Use heuristics*** (*on by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning.
- ***Scan system environment*** (*on by default*): scanning will also check the system areas of your computer.
- ***Enable thorough scanning*** (*off by default):* in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.
- ***Scan for rootkits*** *(on by default):* Anti-Rootkit scan searches your computer for possible rootkits, i.e. programs and technologies that can cover malware activity in your computer. If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

Additional scan settings

The link opens a new ***Additional Scan Settings*** dialog where you can specify the following parameters:



- ***Computer shutdown options*** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option *(Shutdown computer upon scan completion)*, a new option activates that allows the computer to shut down even if it is currently locked *(Force shutdown if computer is locked)*.
- ***File types for scanning*** - you should also decide whether you want to scan:
    - ***All file types*** with the option of defining exceptions from scanning by providing a list of comma

separated file extensions that should not be scanned.

- o ***Selected file types*** - you can specify that you want to scan only files that can be infected *(files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files)*, including media files *(video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus)*. Again, you can specify by extensions which files should always be scanned.

- o Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

Adjust how quickly scan completes

Within this section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the *user sensitive* level of automatic resource usage. If you want the scan to run faster, it will take less time but the system resources used will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease the system resources used by extending the scanning duration.

Set additional scan reports

Click the ***Set additional scan reports ...*** link to open a standalone dialog window called ***Scan reports*** where you can tick several items to define what scan findings should be reported:

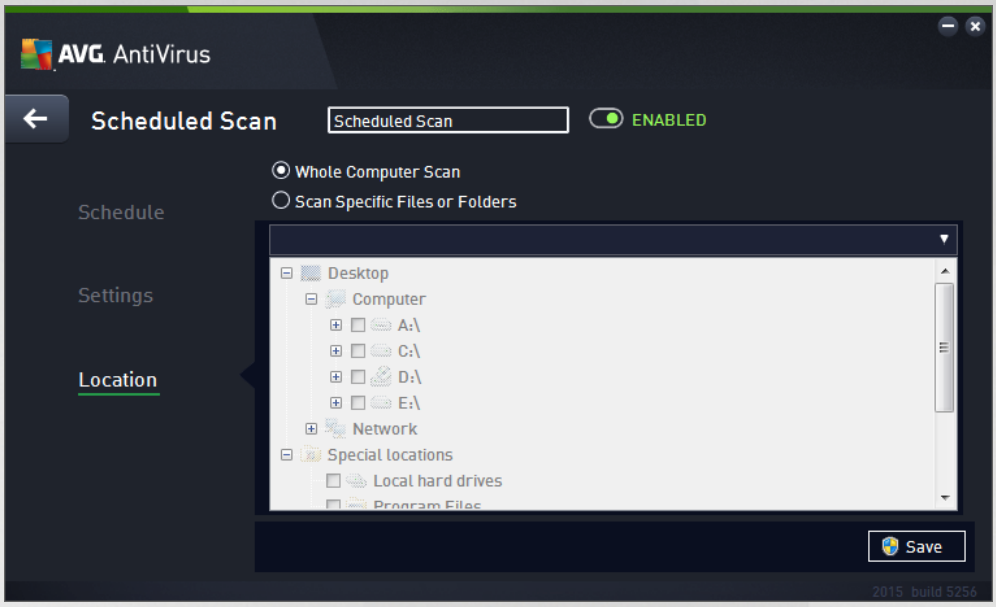


Controls in the dialog

- ***Save*** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.

- - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

8.4.3. Location



On the ***Location*** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. In case you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned (*expand items by clicking the plus node until you find the folder you wish to scan*). You can select multiple folders by checking the respective boxes. The selected folders will appear in the text field on the top of the dialog, and the drop-down menu will keep your selected scan history for later use. Alternatively, you can enter the full path to the desired folder manually (*if you enter multiple paths, it is necessary to separate with semi-colons without extra spaces*).

Within the tree structure you can also see a branch called ***Special locations***. Below is a list of locations that will be scanned once the respective checkbox is marked:

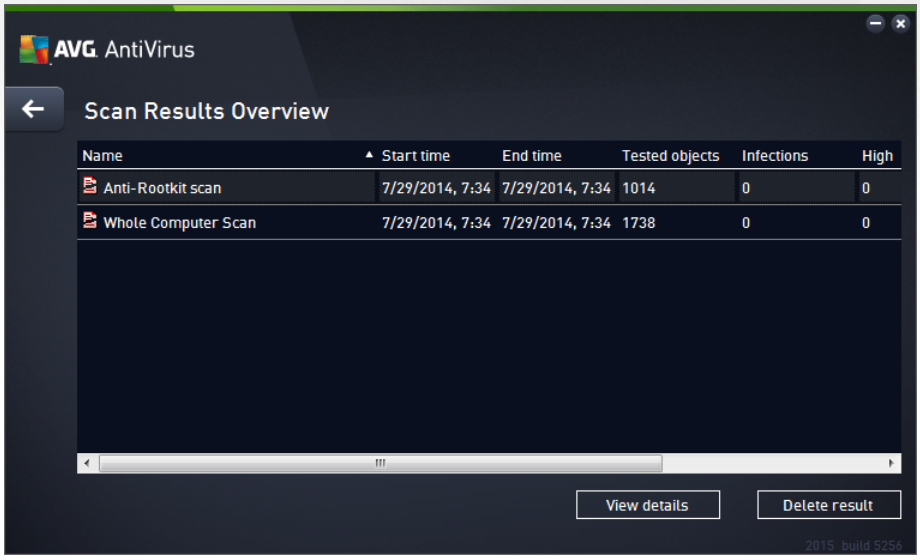
- ***Local hard drives*** - all hard drives of your computer
- ***Program files***
    - C:\Program Files\
    - *in 64-bit version* C:\Program Files (x86)
- ***My Documents folder***
    - *for Win XP:* C:\Documents and Settings\Default User\My Documents\
    - *for Windows Vista/7*: C:\Users\user\Documents\
- ***Shared Documents***
    - *for Win XP*: C:\Documents and Settings\All Users\Documents\
    - *for Windows Vista/7*: C:\Users\Public\Documents\

- ***Windows folder*** - C:\Windows\
- ***Other***
    - *System drive* - the hard drive on which the operating system is installed (usually C:)
    - *System folder* - C:\Windows\System32\
    - *Temporary Files folder* - C:\Documents and Settings\User\Local\ (*Windows XP*); or C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
    - *Temporary Internet Files* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); or C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controls in the dialog

- ***Save*** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.
- - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

8.5. Scan Results



The ***Scan results overview*** dialog provides a list of results of all so far performed scans. The chart provides the following information on each scan result:

- ***Icon*** - The first column displays an information icon describing the status of the scan:
    - No infections found, scan completed

- No infections found, scan was interrupted before completion
- Infections were found and not healed, scan completed
- Infections were found and not healed, scan was interrupted before completion
- Infections found and all were healed or removed, scan completed
- Infections found and all were healed or removed, scan was interrupted before completion

- ***Name*** - The column provides the name of the respective scan. Either it is one of the two predefined scans, or your own scheduled scan.
- ***Start time*** - Gives the exact date and time the scan was launched.
- ***End time*** - Gives the exact date and time the scan finished, was paused, or interrupted.
- ***Tested objects*** - Provides the total number of all objects that were scanned.
- ***Infections*** - Gives the number of removed/total infections found.
- ***High / Medium / Low*** - The subsequent three columns give the number of high, medium and low severity infections found respectively.
- ***Rootkits*** - Provides the total number of rootkits found during the scanning.

Dialog controls

View details - Click the button to see detailed information about a selected scan *(highlighted in the chart above)*.

Delete results - Click the button to remove a selected scan result information from the chart.

- Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

8.6. Scan results details

To open an overview of detailed information on a selected scan result, click the ***View details*** button accessible in the Scan results overview dialog. You will get redirected to the same dialog interface describing in details the information on a respective scan result. The information is divided on three tabs:

- ***Summary*** - The tab gives basic information about the scan: If it was completed successfully, if any threats were found and what happened to them.
- ***Details*** - The tab displays all information about the scan, including details about any detected threats. Export overview to file enables you to save it as a .csv file.
- ***Detections*** - This tab is only displayed if there were any threats detected during the scan, and gives detailed information about the threats:

 ***Information severity***: information or warnings, not real threats. Typically documents containing macros, documents or archives protected by a password, locked files, etc.

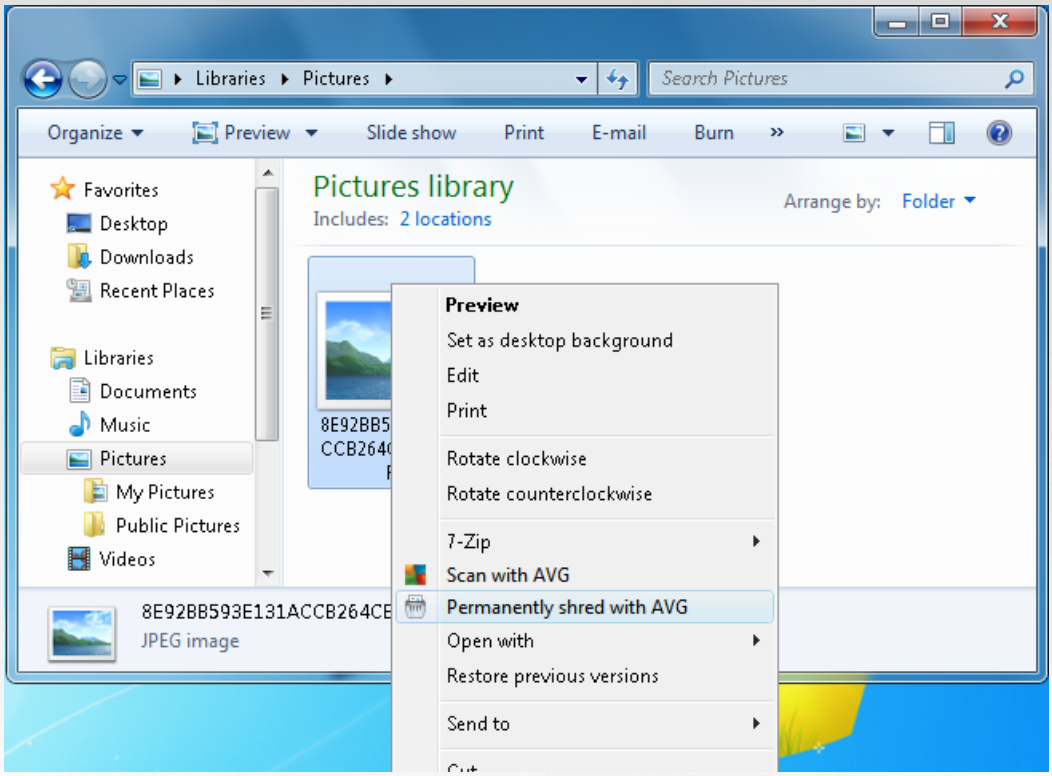
 ***Medium severity***: typically potentially unwanted applications *(such as adware)* or tracking cookies

 ***High severity***: serious threats such as viruses, Trojans, exploits, etc. Also objects detected by the Heuristics detection method, i.e. threats not yet described in the virus database.

9. AVG File Shredder

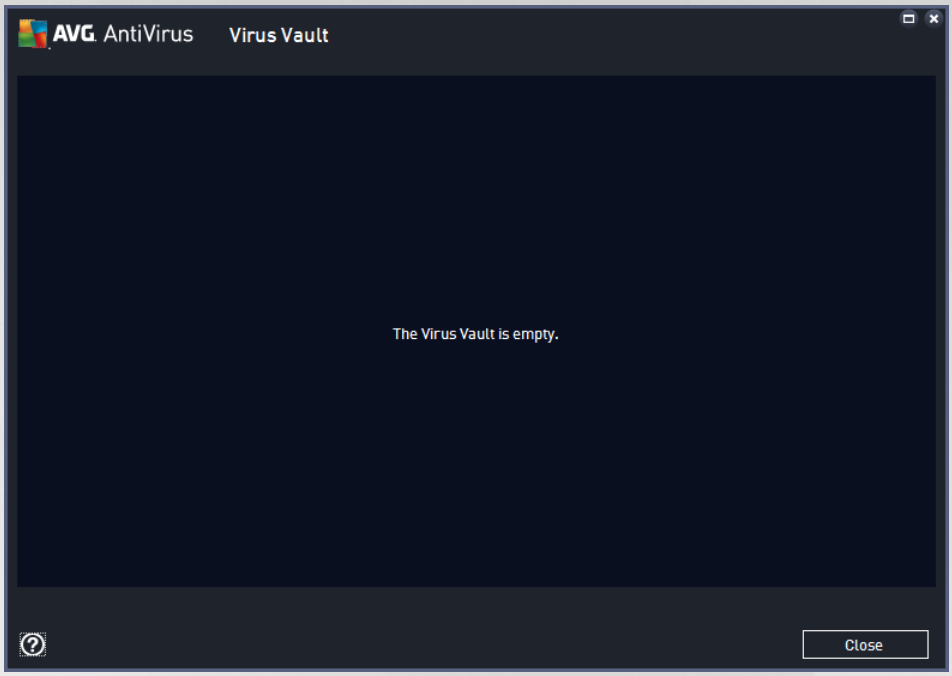
AVG File Shredder has been designed to delete files absolutely securely, that is with no chance to recover them, even with advanced software tools for this purpose.

To shred a file or folder, right-click it in a file manager *(Windows Explorer, Total Commander, ...)* and select ***Permanently shred with AVG*** in the context menu. Files in the Recycle Bin can be shredded as well. If a specific file in a specific location *(e.g. CD-ROM)* cannot be shredded reliably, you will be notified, or the option in the context menu will not be available at all.



Please always bear in mind: Once you shred a file, it is gone forever.

10. Virus Vault



Virus Vault is a safe environment for the management of suspect/infected objects detected during AVG tests. Once an infected object is detected during scanning, and AVG is not able to heal it automatically, you are asked to decide what is to be done with the suspect object. The recommended solution is to move the object to the ***Virus Vault*** for further treatment. The main purpose of the ***Virus Vault*** is to keep any deleted file for a certain period of time, so that you can make sure you do not need the file any more in its original location. Should you find out that the file absence causes problems, you can send the file in question to analysis, or restore it to the original location.

The ***Virus vault*** interface opens in a separate window and offers an overview of the information on quarantined infected objects:

- ***Date Added*** - Provides date and time the suspected file was detected and removed to the Virus Vault.
- ***Threat*** - In case you decided to install the Identity component within your **AVG AntiVirus 2015**, a graphical identification of the finding severity will be provided in this section: from unobjectionable *(three green dots)* up to very dangerous *(three red dots)*. Also you will find information on the infection type and its original location. The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia.
- ***Source*** - Specifies which component of **AVG AntiVirus 2015** has detected the respective threat.
- ***Notifications*** - In a very rare situation, some notes may occur in this column providing detailed comments on the respective detected threat.

Control buttons

The following control buttons are accessible from the ***Virus Vault*** interface:

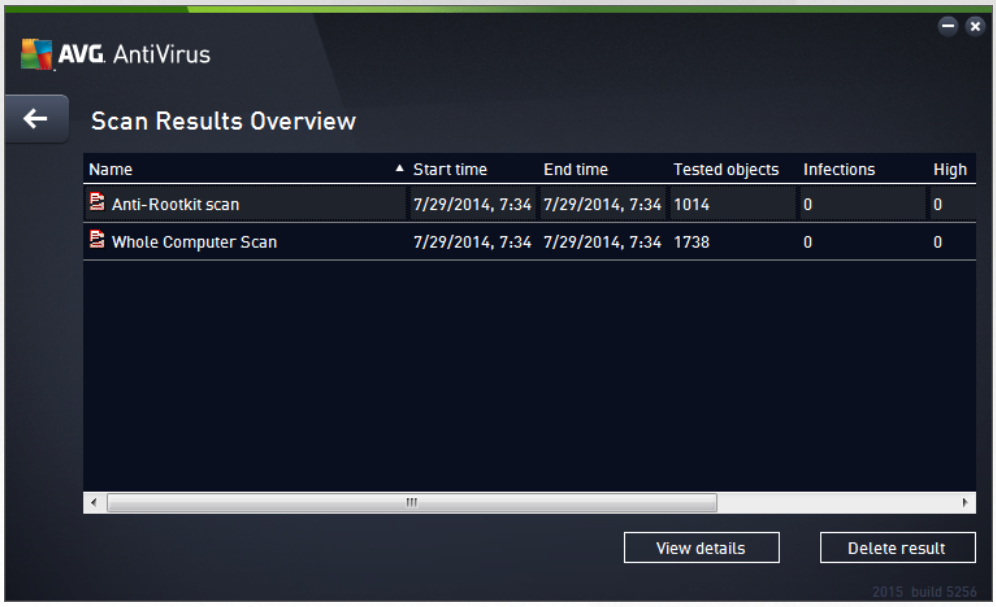
- ***Restore*** - removes the infected file back to its original location on your disk.
- ***Restore As*** - moves the infected file to a selected folder.
- ***Send to analysis*** - the button is only active when you highlight an object in the list of detections above. In such case, you have the option to send the selected detection to the AVG virus labs for further detailed analysis. Please note that this feature should primarily serve for sending false positives, i.e. files that have been detected by AVG as infected or suspicious, but which you believe are harmless.
- ***Details*** - for detailed information on the specific threat quarantined in the ***Virus Vault*** highlight the selected item in the list and click the ***Details*** button to call a new dialog with a description of the detected threat.
- ***Delete*** - removes the infected file from the ***Virus Vault*** completely and irreversibly.
- ***Empty Vault*** - removes all ***Virus Vault*** content completely. By removing the files from the ***Virus Vault***, these files are irreversibly removed from the disk (*not moved to the recycle bin*).

11. History

The ***History*** section includes information on all past events *(such as updates, scans, detections, etc.)* and reports about these events. This section is accessible from the main user interface via the ***Options / History*** item. Further, the history of all recorded events is divided into the following parts:

- Scan Results
- Resident Shield Results
- Email Protection Results
- Online Shield Results
- Event History

11.1. Scan results



The ***Scan results overview*** dialog is accessible via the ***Options / History / Scan results*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window. The dialog provides a list of all previously launched scans and information on their results:

- ***Name*** - scan designation; it can either be the name of one of the predefined scans, or a name you have given to your own scheduled scan. Every name includes an icon indicating the scan result:

  - green icon informs there was no infection detected during the scan

  - blue icon announces there was an infection detected during the scan but the infected object was removed automatically

  - red icon warns there was an infection detected during the scan and it could not be removed!

Each icon can either be solid or cut in half - the solid icons stands for a scan that was completed and finished properly; the cut-in-half icon means the scan was canceled or interrupted.

Note: *For detailed information on each scan please see the Scan Results dialog accessible via the View details button (in the bottom part of this dialog).*

- ***Start time*** - date and time when the scan was launched
- ***End time*** - date and time when the scan ended
- ***Tested objects*** - number of objects that were checked during scanning
- ***Infections*** - number of virus infections detected / removed
- ***High / Medium*** - these columns give the number of removed/total infections found of high, and medium severity respectively
- ***Info*** - information relating to the scanning course and result *(typically on its finalization or interruption)*
- ***Rootkits*** - number of detected rootkits

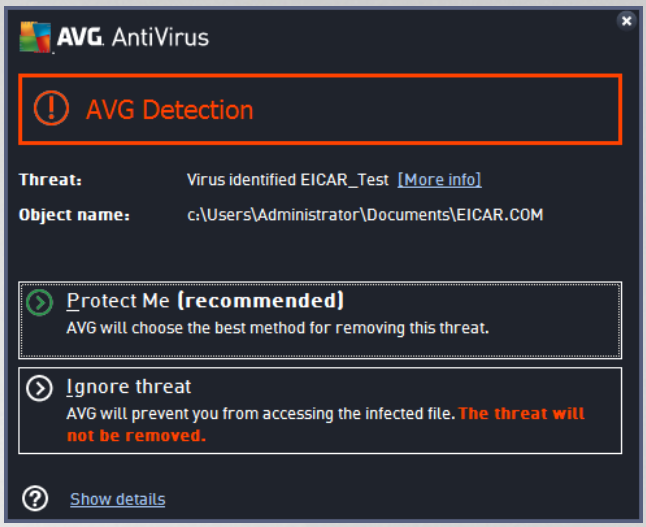
Control buttons

The control buttons for the ***Scan results overview*** dialog are:

- ***View details*** - press it to switch to the Scan results dialog to view detailed data on the selected scan
- ***Delete result*** - press it to remove the selected item from the scan results overview
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog

11.2. Resident Shield Results

The ***Resident Shield*** service is a part of the ***Computer*** component and scans files as they are copied, opened, or saved. When a virus or any kind of threat is detected, you will be warned immediately via the following dialog:



Within this warning dialog you will find information on the object that was detected and assigned as infected (*Threat*), and some descriptive facts on the recognized infection (*Description*). The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia, if these are known. In the dialog, you will also see an overview of available solutions on how to treat the detected threat. One of the alternatives will be labeled as recommended: ***Protect Me (recommended). If possible, you should always stick to this option!***

Note: *It may happen that the size of the detected object exceeds the free space limit in the Virus Vault. If so, a warning message pops up informing you about the issue as you try to move the infected object to the Virus Vault. However, the Virus Vault size can be modified. It is defined as an adjustable percentage of the real size of your hard disk. To increase the size of your Virus Vault, go to the Virus Vault dialog within the AVG Advanced Settings, via the 'Limit Virus Vault size' option.*

In the bottom section of the dialog you can find the ***Show details*** link. Click it to open a new window with detailed information on the process running while the infection was detected, and the process' identification.

A list of all Resident Shield detections is available for overview within the ***Resident Shield detection*** dialog. This dialog is accessible via the ***Options / History / Resident Shield detection*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window. The dialog offers an overview of objects that were detected by the resident shield evaluated as dangerous and either cured or moved to the Virus Vault.



For each detected object the following information is provided:

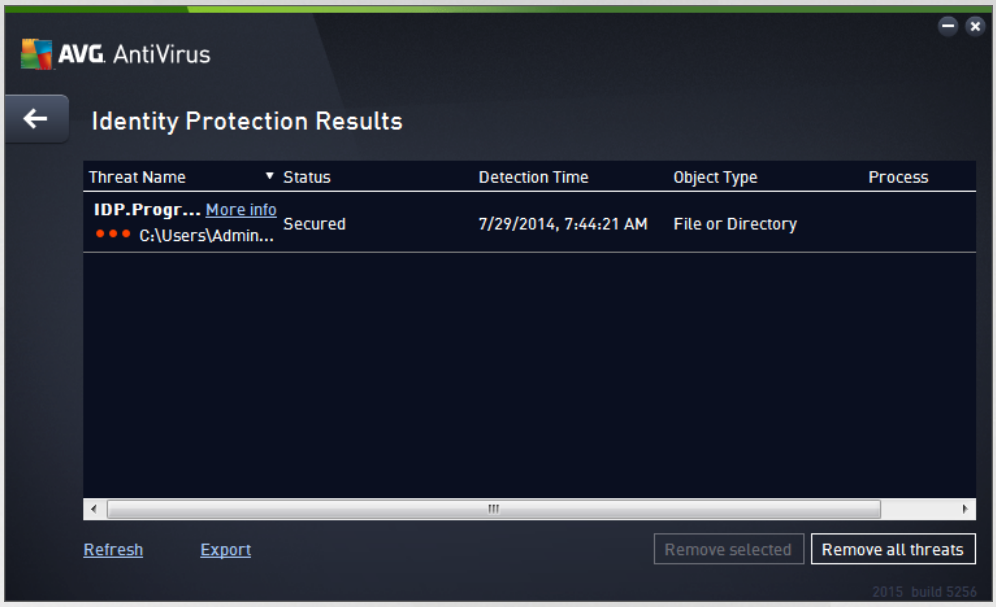
- ***Threat Name*** - description (*possibly even name*) of the detected object and its location. The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia.
- ***Status*** - action performed with the detected object
- ***Detection Time*** - date and time the threat was detected and blocked
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

Control buttons

- ***Refresh*** - update the list of findings detected by ***Online Shield***
- ***Export*** - export the entire list of detected objects in a file
- ***Remove selected*** - in the list you can highlight selected records, and use this button to delete just these selected items
- ***Remove all threats*** - use the button to delete all records listed in this dialog
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog

11.3. Identity Protection Results

The ***Identity Protection Results*** dialog is accessible via the ***Options / History / Identity Protection Results*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window.



The dialog provides a list of all findings detected by the Identity Protection component. For each detected object the following information is provided:

- ***Threat Name*** - description *(possibly even name)* of the detected object and its location. The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia.
- ***Status*** - action performed with the detected object
- ***Detection Time*** - date and time the threat was detected and blocked
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

In the bottom part of the dialog, below the list, you will find information on total number of detected objects listed above. You can also export the entire list of detected objects in a file (***Export list to file***) and delete all entries on detected objects (***Empty list***).

Control buttons

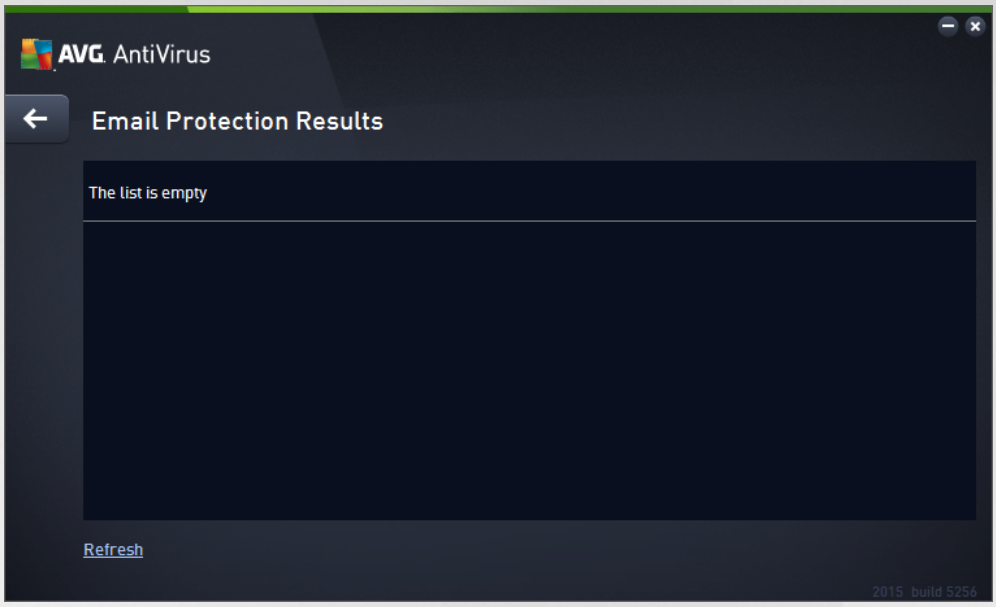
The control buttons available within the ***Identity Protection Results*** interface are as follows:

- ***Refresh list*** - updates the list of detected threats
- ← - to switch back to the default AVG main dialog *(components overview)*, use the arrow in the

upper left-hand corner of this dialog

11.4. Email Protection Results

The ***Email Protection Results*** dialog is accessible via the ***Options / History / Email Protection Results*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window.



The dialog provides a list of all findings detected by the Email Scanner component. For each detected object the following information is provided:

- ***Detection name*** - description *(possibly even name)* of the detected object, and its source
- ***Result*** - action performed with the detected object
- ***Detection time*** - date and time the suspicious object was detected
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

In the bottom part of the dialog, below the list, you will find information on total number of detected objects listed above. You can also export the entire list of detected objects in a file (***Export list to file***) and delete all entries on detected objects (***Empty list***).

Control buttons

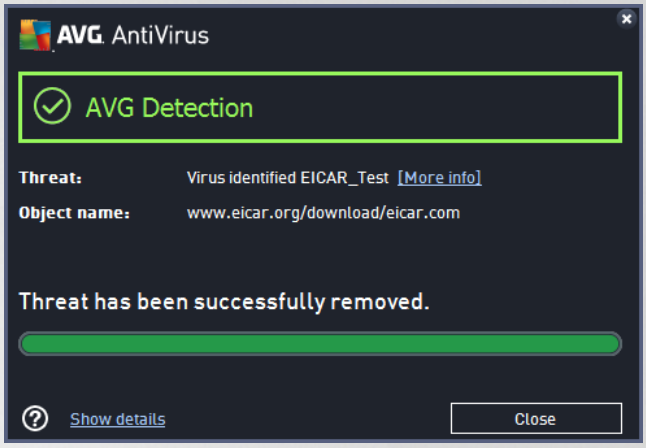
The control buttons available within the ***Email Scanner detection*** interface are as follows:

- ***Refresh list*** - updates the list of detected threats
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the

upper left-hand corner of this dialog

11.5. Online Shield Results

Online Shield scans the content of visited web pages and possible files included in them even before these are displayed in your web browser or downloaded to your computer. If a threat is detected, you will be warned immediately with the following dialog:



Within this warning dialog you will find information on the object that was detected and assigned as infected (*Threat*), and some descriptive facts on the recognized infection (*Object name*). The *More info* link will redirect you to the online virus encyclopedia where you can find detailed information on the detected infection, if these are known. The dialog provides the following control elements:

- ***Show details*** - click the link to open a new pop-up window where you can find information on the process running while the infection was detected, and the process' identification.
- ***Close*** - click the button to close the warning dialog.

The suspicious web page will not be opened, and the threat detection will be logged in the list of ***Online Shield findings***. This overview of detected threats is accessible via the ***Options / History / Online Shield findings*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window.



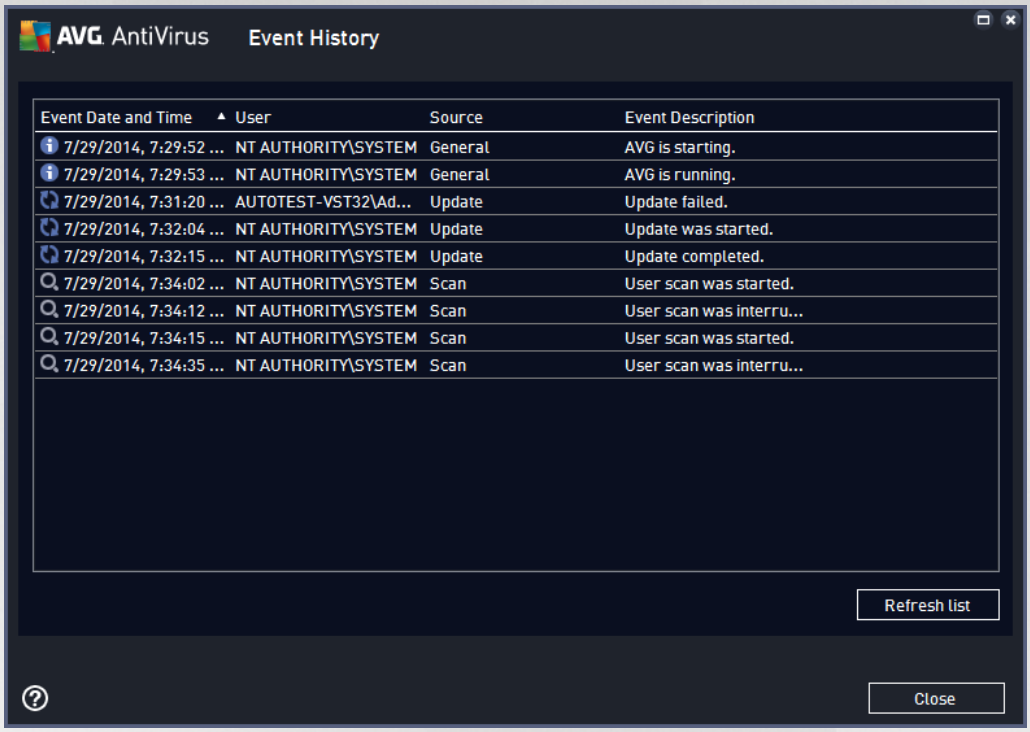
For each detected object the following information is provided:

- ***Threat Name*** - description (*possibly even name*) of the detected object, and its source (*web page*); the *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia.
- ***Status*** - action performed with the detected object
- ***Detection Time*** - date and time the threat was detected and blocked
- ***Object Type*** - type of the detected object

Control buttons

- ***Refresh*** - update the list of findings detected by ***Online Shield***
- ***Export*** - export the entire list of detected objects in a file
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog

11.6. Event History



The ***Event history*** dialog is accessible via the ***Options / History / Event History*** menu item in the upper line navigation of the **AVG AntiVirus 2015** main window. Within this dialog you can find a summary of important events that occurred during **AVG AntiVirus 2015** operation. The dialog provides records of the following types of events: information about updates of the AVG application; information on scanning start, end, or stop (*including automatically performed tests*); information on events connected with virus detection (*either by the resident shield or scanning*) including occurrence location; and other important events.

For each event, the following information is listed:

- ***Event Date and Time*** gives the exact date and time the event occurred.
- ***User*** states the name of the user currently logged in at the time that the event occurred.
- ***Source*** gives information about a source component or other part of the AVG system that triggered the event.
- ***Event Description*** gives a brief summary of what actually happened.

Control buttons

- ***Refresh list*** - press the button to updates all entries in the list of events
- ***Close*** - press the button to return to the **AVG AntiVirus 2015** main window

12. AVG Updates

No security software can guarantee true protection from various types of threats unless it is regularly updated! Virus writers are always looking for new flaws that they can exploit in both software and operating systems. New viruses, new malware, new hacking attacks appear daily. For this reason, software vendors are continually issuing updates and security patches, to fix any security holes that are discovered.

Considering all the newly-emerged computer threats and the speed at which they spread, it is absolutely crucial to update your **AVG AntiVirus 2015** regularly. The best solution is to stick to the program default settings where the automatic update is configured. Please bear in mind that if the virus database of your **AVG AntiVirus 2015** is not up-to-date, the program will not be able to detect the latest threats!

It is crucial to update your AVG regularly! Essential virus definition updates should be daily if possible. Less urgent program updates can be weekly.

12.1. Update launch

To provide the maximum security available, **AVG AntiVirus 2015** is by default scheduled to look for new virus database updates every four hours. Since AVG updates are not released according to any fixed schedule but rather in response to the amount and severity of new threats, this check-up is highly important to make sure your AVG virus database is kept up-to-date all the time.

If you want to check the new update files immediately, use the Update now quick link in the main user interface. This link is available at all times from any user interface dialog. Once you start the update, AVG will first verify whether there are new update files available. If so, **AVG AntiVirus 2015** starts to download them and launches the update process itself. You will be informed about the update results in the slide dialog over the AVG system tray icon.

Should you wish to reduce the number of update launches, you can set up your own update launch parameters. However, ***it is strictly recommended that you launch the update at least once a day!*** The configuration can be edited within the Advanced settings/Schedules section, specifically in the following dialogs:

- Definitions update schedule
- Program update schedule

12.2. Update levels

AVG AntiVirus 2015 offers two update levels to select from:

- ***Definitions update*** contains changes necessary for reliable antivirus protection. Typically, it does not include any changes to the code and updates only the definition database. This update should be applied as soon as it is available.
- ***Program update*** contains various program changes, fixes, and improvements.

When scheduling an update, it is possible to define specific parameters for both update levels:

- Definitions update schedule
- Program update schedule

Note: *If a scheduled program update and scheduled scan coincides, the update process is of higher priority and the scan will be interrupted.In such a case you will be informed about the collision.*

13. FAQ and Technical Support

Should you have any sales or technical trouble with your **AVG AntiVirus 2015** application, there are several ways to obtain help. Please chose from the following options:

- ***Get Support***: Right within the AVG application you can reach a dedicated customer support page on the AVG website (*http://www.avg.com/*). Select the ***Help / Get Support*** main menu item to get redirected to the AVG website with available support avenues. To proceed, please follow the instructions on the web page.

- ***Support*** *(main menu link)*: The AVG application menu (*on top of the main user interface*) includes the ***Support*** link that opens a new dialog with all types of information you might need when trying to find help. The dialog includes basic data on your installed AVG program (*program / database version*), license details, and a list of quick support links.

- ***Troubleshooting in help file***: A new ***Troubleshooting*** section is available directly in the help file included with **AVG AntiVirus 2015** *(to open the help file, press F1 key in any dialog in the application)*. This section provides a list of the most frequently occurring situations when a user desires to look up professional help for a technical issue. Please select the situation that best describes your problem, and click it to open detailed instructions leading to the problem solution.

- ***AVG website support center***: Alternatively, you can look up the solution to your problem on the AVG website (*http://www.avg.com/*). In the ***Support*** section you can find an overview of thematic groups dealing with both sales and technical issues, a structured section of frequently asked questions, and all available contacts.

- ***AVG ThreatLabs***: A specific AVG related website (*http://www.avg.com/about-viruses*) is dedicated to virus issues providing structured overview of information related to online threats. You can also find instructions on removing viruses, spyware, and advice on how to stay protected.

- ***Discussion forum***: You can also use the AVG users discussion forum at http://community.avg.com/.